CHAPTER 1

Bialgebras and Hopf algebras

We define bialgebras, Hopf Algebras, and related algebraic structures, largely following the original paper [**?**] of Milnor and Moore but incorporating various simplifications and amplifications. The reader is urged to recall our conventions on grading and commutativity from **??**. The theme is the definition of algebraic structures by use of dual commutative diagrams. Thus the familiar concepts of algebra and module dualize to concepts of coalgebra and comodule, and the structures of algebra and coalgebra combine to give the notion of a bialgebra. Incorporating antipodes (sometimes called conjugations), we obtain the notion of a Hopf algebra. In the cocommutative case, bialgebras and Hopf algebras can be viewed as monoids and groups in the symmetric monoidal category of cocommutative coalgebras.

1. Preliminaries

We shall work over a commutative ground ring R. The reader may prefer to take R to be a field, since that holds in most applications. Unless otherwise specified, $\otimes = \otimes_R$ and $\mathrm{Hom} = \mathrm{Hom}_R$. Recall that these are defined on graded R-modules by

$$(A\otimes B)_n = \sum_{i+j=n} A_i \otimes B_j \quad \text{and} \quad \mathrm{Hom}_n(A,B) = \prod_i \mathrm{Hom}(A_i, B_{i+n}).$$

We think of R, or any other ungraded R-module, as concentrated in degree 0. We define the dual A^* of A by $A^* = \mathrm{Hom}(A,R)$, so that $A^n = \mathrm{Hom}(A_n, R)$; here we have implicitly reversed the grading to superscripts (with a sign change).

Of course, $\otimes$ is associative and unital (with unit R) up to natural isomorphism and has the natural commutativity isomorphism

$$\gamma : A\otimes B \to B\otimes A$$

specified by $\gamma(a\otimes b) = (-1)^{\deg a \deg b} b\otimes a$. We introduce such a sign whenever two entities are permuted. By a harmless standard abuse, we omit the unit and associativity isomorphisms from diagrams and treat them as if they were identifications. Use of the commutativity isomorphism is always made explicit. In categorical language, the category $\mathscr{M}_R$ of graded R-modules is symmetric monoidal, and it is closed in the sense that there is a natural isomorphism

$$\mathrm{Hom}(A\otimes B, C) \cong \mathrm{Hom}(A, \mathrm{Hom}(B,C));$$

it sends f to g, where $g(a)(b) = f(a\otimes b)$. There are further natural maps

$$\nu\colon\ \mathrm{Hom}(A,B)\otimes C \to \mathrm{Hom}(A, B\otimes C),$$

$$\rho\colon\ A \to A^{**},$$

and

$$\alpha\colon\ \mathrm{Hom}(A,C)\otimes \mathrm{Hom}(B,D) \longrightarrow \mathrm{Hom}(A\otimes B, C\otimes D),$$

which specializes to

$$\alpha\colon A^* \otimes B^* \to (A \otimes B)^*.$$

These maps are specified by

$$\nu(f \otimes c)(a) = (-1)^{deg(c)deg(a)} f(a) \otimes c,$$

$$\rho(a)(f) = (-1)^{\deg(a)\deg(f)} f(a),$$

and

$$\alpha(f \otimes g)(a \otimes b) = (-1)^{\deg(g)\deg(b)} f(a)g(b).$$

We say that A is projective if each A_i is projective (over R), and we say that A is of finite type if each A_i is finitely generated (over R). We say that A is bounded if it is non-zero in only finitely many degrees. Thus A is finitely generated if and only if it is bounded and of finite type. We say that A is bounded below (or above) if $A_i = 0$ for i sufficiently small (or large). Then ν is an isomorphism if A is bounded and either A or C is projective of finite type, ρ is an isomorphism if A is projective of finite type, and the last map α is an isomorphism if A and B are bounded below and A or B is projective of finite type. In these assertions, boundedness hypotheses ensure that the products appearing in our Hom's are finite, so that they become sums, and projective of finite type hypotheses allow us to apply the analogous assertions for ungraded modules. Henceforward, we implicitly restrict attention to non-negatively graded modules, for which $A_i = 0$ if $i < 0$, since that is the case of greatest interest in algebraic topology.

Virtually all of our substantive results will be proven by use of filtrations and bigraded modules. We shall usually have $A_{p,q} = 0$ for all $p < 0$ or all $p > 0$. The signs occurring in the study of bigraded modules always refer to the total degree $p + q$. The tensor product of bigraded modules is given by

$$(A \otimes B)_{p,q} = \sum_{i+j=p,k+l=q} A_{i,k} \otimes B_{j,l}.$$

Similarly, the dual A^* is given by $A^{p,q} = \mathrm{Hom}(A_{p,q}, R)$.

A filtration $\{F_pA\}$ of a graded module A is an expanding sequence of submodules F_pA. A filtration is said to be complete if

$$A \cong \mathrm{colim} F_pA \quad \text{and} \quad A \cong \lim A/F_pA$$

In most cases that we shall encounter, we shall have either $F_pA = A$ for $p \geq 0$ and $\cap_p F_pA = 0$ or $F_pA = 0$ for $p < 0$ and $A = \cup_p F_pA$. In such cases, completeness is clear. We give R the trivial filtration, $F_pR = 0$ for $p < 0$ and $F_pR = R$ for $p \geq 0$. The tensor product of filtered modules is filtered by

$$F_p(A \otimes B) = \mathrm{Im}\left(\sum_{i+j=p} F_iA \otimes F_jB\right) \subset A \otimes B.$$

We say that a filtration of A is flat if each A/F_pA is a flat R-module; we say that a filtration is split if each sequence

$$0 \to F_pA \to A \to A/F_pA \to 0$$

is split exact over R. Of course, these both hold automatically when R is a field.

The associated bigraded module E^0A of a filtered module A is specified by

$$E^0_{p,q}A = (F_pA/F_{p-1}A)_{p+q}.$$

Of course, E^0 is a functor from filtered modules to bigraded modules.

PROPOSITION 1.1. *Let $f : A \to B$ be a map of complete filtered R-modules. If $E^0 f : E^0 A \to E^0 B$ is a monomorphism, or an epimorphism, or an isomorphism, then f and all its restrictions $F_p f$ are also monomorphisms, or epimorphisms, or isomorphisms.*

PROOF. The commutative diagrams

$$\begin{tikzcd}
0 \arrow[r] & F_pA/F_{p-1}A \arrow[r] \arrow[d] & F_qA/F_{p-1}A \arrow[r] \arrow[d] & F_qA/F_pA \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F_pB/F_{p-1}B \arrow[r] & F_qB/F_{p-1}B \arrow[r] & F_qB/F_pB \arrow[r] & 0
\end{tikzcd}$$

imply inductively that f induces a monomorphism or epimorphism or isomorphism $F_qA/F_pA \to F_qB/F_pB$ for all $p < q$. Passing to colimits over q, we find that the same is true for $A/F_pA \to B/F_pB$ for all p. Since lim is left exact and preserves isomorphisms, we obtain the conclusions for the monomorphism and isomorphism cases by passage to limits. Since lim is not right exact, we must work a little harder in the epimorphism case. Here we let C_p be the kernel of the epimorphism $A/F_pA \to B/F_pB$ and let $C = \lim C_p$. A chase of the commutative exact diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & F_{p+1}A/F_pA \arrow[r] \arrow[d] & F_{p+1}B/F_pB \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C_p \arrow[r] \arrow[d] & A/F_pA \arrow[r] \arrow[d] & B/F_pB \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C_{p+1} \arrow[r] & A/F_{p+1}A \arrow[r] \arrow[d] & B/F_{p+1}B \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

shows that $\{C_p\}$ is an inverse system of epimorphisms. Therefore $\lim^1 C_p = 0$ and each map $C \to C_p$ is an epimorphism. The exact sequence of inverse systems

$$0 \to \{C_p\} \to \{A/F_pA\} \to \{B/F_pB\} \to 0$$

gives rise to an exact sequence $0 \to C \to A \to B \to 0$ and a chase of the commutative exact diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & C \arrow[r] \arrow[d] & C_p \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F_pA \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & A/F_pA \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F_pB \arrow[r] & B \arrow[r] \arrow[d] & B/F_pB \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

shows that $F_pA \to F_pB$ is an epimorphism. □

Chases of congeries of exact sequences give the following comparison assertion.

Proposition 1.2. *Let A and B be filtered R-modules such that A and B are either both split or both flat. Then the natural map*

$$E^0A \otimes E^0B \to E^0(A \otimes B)$$

is an isomorphism of bigraded R-modules.

2. Algebras, coalgebras, and bialgebras

We give the most basic definitions in this section.

Definition 2.1. An R-algebra $A = (A, \phi, \eta)$ is a graded R-module A together with a product $\phi : A \otimes A \to A$ and unit $\eta : R \to A$ such that the following diagrams commute.

$$\begin{tikzcd}
A \otimes A \otimes A \arrow[r, "\mathrm{id} \otimes \phi"] \arrow[d, "\phi \otimes \mathrm{id}"'] & A \otimes A \arrow[d, "\phi"] \\
A \otimes A \arrow[r, "\phi"'] & A
\end{tikzcd} \quad \text{and} \quad \begin{tikzcd}
A \otimes R \arrow[r, "\mathrm{id} \otimes \eta"] \arrow[dr, equal] & A \otimes A \arrow[d, "\phi"] & R \otimes A \arrow[l, "\eta \otimes \mathrm{id}"'] \arrow[dl, equal] \\
 & A &
\end{tikzcd} .$$

A is commutative if the following diagram also commutes.

$$\begin{tikzcd}
A \otimes A \arrow[rr, "\gamma"] \arrow[dr, "\phi"'] & & A \otimes A \arrow[dl, "\phi"] \\
 & A &
\end{tikzcd}$$

An augmentation of A is a morphism of algebras $\varepsilon : A \to R$. Given ε, $\ker \varepsilon$ is denoted IA and called the augmentation ideal of A; since $\varepsilon\eta = \mathrm{id}$, $A \cong R \oplus IA$. If A and B are algebras, then so is $A \otimes B$; its unit and product are

$$R = R \otimes R \xrightarrow{\eta \otimes \eta} A \otimes B \qquad \text{and} \qquad A \otimes B \otimes A \otimes B \xrightarrow{(\phi \otimes \phi)(\mathrm{id} \otimes \gamma \otimes \mathrm{id})} A \otimes B.$$

An algebra A is commutative if and only if $\phi : A \otimes A \to A$ is a map of algebras.

Definition 2.2. An R-coalgebra $C = (C, \psi, \varepsilon)$ is a graded R-module C together with a coproduct $\psi : C \to C \otimes C$ and counit (or augmentation) $\varepsilon : C \to R$ such that the following diagrams commute.

$$\begin{tikzcd} C \arrow[r, "\psi"] \arrow[d, "\psi"'] & C \otimes C \arrow[d, "\mathrm{id} \otimes \psi"] \\ C \otimes C \arrow[r, "\psi \otimes \mathrm{id}"'] & C \otimes C \otimes C \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} & C \arrow[dl, equal] \arrow[d, "\psi"] \arrow[dr, equal] & \\ C \otimes R & C \otimes C \arrow[l, "\mathrm{id} \otimes \varepsilon"] \arrow[r, "\varepsilon \otimes \mathrm{id}"'] & R \otimes C \end{tikzcd}$$

C is cocommutative if the following diagram also commutes.

$$\begin{tikzcd} & C \arrow[dl, "\psi"'] \arrow[dr, "\psi"] & \\ C \otimes C \arrow[rr, "\gamma"'] & & C \otimes C. \end{tikzcd}$$

A unit (sometimes called coaugmentation) for C is a morphism of coalgebras $\eta : R \to C$; given η, define $JC = \operatorname{coker} \eta$. Since $\varepsilon\eta = \mathrm{id}$, $C \cong R \oplus JC$. If C and D coalgebras, then so is $C \otimes D$; its augmentation and coproduct are

$$C \otimes B \xrightarrow{\varepsilon \otimes \varepsilon} R \otimes R = R \qquad \text{and} \qquad C \otimes D \xrightarrow{(\mathrm{id} \otimes \gamma \otimes \mathrm{id})(\psi \otimes \psi)} C \otimes D \otimes C \otimes D.$$

A coalgebra C is cocommutative if and only if ψ is a map of coalgebras.

Definition 2.3. Let A be a flat R-module. A bialgebra $(A, \phi, \psi, \eta, \varepsilon)$ is an algebra (A, ϕ, η) with augmentation ε and a coalgebra (A, ψ, ε) with unit η such that the following diagram is commutative.

$$\begin{tikzcd} A \otimes A \arrow[r, "\phi"] \arrow[d, "\psi \otimes \psi"'] & A \arrow[r, "\psi"] & A \otimes A \\ A \otimes A \otimes A \otimes A \arrow[rr, "\mathrm{id} \otimes \gamma \otimes \mathrm{id}"'] & & A \otimes A \otimes A \otimes A \arrow[u, "\phi \otimes \phi"'] \end{tikzcd}$$

That is, ϕ is a morphism of coalgebras or, equivalently, ψ is a morphism of algebras. If the associativity of ϕ and coassociativity of ψ are deleted from the definition, then A is said to be a quasi bialgebra[1]. There result notions of coassociative quasi bialgebra and of associative quasi bialgebra.

The flatness of A is usually not assumed but holds in practice; in its absence, the notion of bialgebra is perhaps too esoteric to be worthy of contemplation.

Lemma 2.4. *Let A be projective of finite type.*

(i) (A, ϕ, η) is an algebra if and only if (A^*, ϕ^*, η^*) is a coalgebra, ε is an augmentation of A if and only if ε^* is a unit of A^*, and A is commutative if and only if A^* is cocommutative.

(ii) $(A, \phi, \psi, \eta, \varepsilon)$ is a bialgebra if and only if $(A^*, \phi^*, \psi^*, \eta^*, \varepsilon^*)$ is a bialgebra.

Similar conclusions hold for quasi bialgebras, and so forth.

Definition 2.5. We define indecomposable and primitive elements.

[1] This use of "quasi" is due to Milnor and Moore [**?**]; Drinfeld later gave a more precise meaning to the term quasi-Hopf algebra [**?**].

(i) Let A be an augmented algebra. Define the R-module QA of indecomposable elements of A by the exact sequence

$$\begin{tikzcd} IA\otimes IA \arrow[r, "\phi"] & IA \arrow[r] & QA \arrow[r] & 0. \end{tikzcd}$$

Note that QA is well-defined even if A is not associative.

(ii) Let C be a unital coalgebra. Define the R-module PC of primitive elements of C by the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & PC \arrow[r] & JC \arrow[r, "\psi"] & JC\otimes JC. \end{tikzcd}$$

Let $IC = \ker\varepsilon$. We say that $x\in IC$ is primitive if its image in JC lies in PC. Note that PC is well-defined even if C is not coassociative.

Lemma 2.6. *If C is a unital coalgebra and $x\in IC$, then*

$$\psi(x) = x\otimes 1 + \sum x'\otimes x'' + 1\otimes x,$$

where $\sum x'\otimes x''\in IC\otimes IC$. If x is primitive, then

$$\psi(x) = x\otimes 1 + 1\otimes x.$$

Proof. $C\otimes C = (R\otimes R)\oplus(IC\otimes R)\oplus(R\otimes IC)\oplus(IC\otimes IC)$, where $R = \operatorname{Im}\eta$, and the natural map $IC\to JC$ is an isomorphism. The first statement holds since

$$(\varepsilon\otimes\mathrm{id})\psi(x) = x = (\mathrm{id}\otimes\varepsilon)\psi(x),$$

and the second statement is immediate from the definition. □

When $x\in IC$, we usually write $\psi(x) = \sum x'\otimes x''$ generically for the coproduct[2], including the terms $x\otimes 1$ and $1\otimes x$ and omitting an index of summation.

Lemma 2.7. *If A is an augmented algebra, then $P(A^*) = (QA)^*$. If, further, A is projective of finite type, then*

$$\begin{tikzcd} IA\otimes IA \arrow[r] & IA \arrow[r] & QA \arrow[r] & 0 \end{tikzcd}$$

is split exact if and only if

$$\begin{tikzcd} 0 \arrow[r] & P(A^*) \arrow[r] & I(A^*) \arrow[r] & I(A^*)\otimes I(A^*) \end{tikzcd}$$

is split exact; when this holds, $P(A^*)^* = QA$.

Definition 2.8. Let A be a quasi bialgebra. Define $\nu : PA\to QA$ to be the composite

$$\begin{tikzcd} PA \arrow[r] & JA\cong IA \arrow[r] & QA \end{tikzcd}$$

(or, equivalently, the restriction of $IA\to QA$ to PA if PA is regarded as contained in A). A is said to be primitive, or primitively generated, if ν is an epimorphism; A is said to be coprimitive if ν is a monomorphism.

A structure A (algebra, coalgebra, bialgebra, etc) is filtered if it has a split filtration such that all of the structure maps preserve filtration. It follows that E^0A is a structure of the given type. The following definitions give basic tools for the study of (quasi) bialgebras by passage to associated bigraded primitive or coprimitive bialgebras. We warn the reader that the filtrations in the following two definitions are not necessarily complete. In the first case, that is a familiar fact

[2] In the algebraic literature, the more usual convention is to write $\psi(x) = \sum x_{(1)}\otimes x_{(2)}$.

from classical algebra since the intersection of the powers of a (two-sided) ideal in a ring can be non-zero [**?**, p. 110].

Definition 2.9. Let A be an augmented algebra. Define the product filtration $\{F_pA\}$ by $F_pA = A$ if $p \geq 0$ and $F_pA = (IA)^{-p}$ if $p < 0$. Observe that

$$E^0_{p,*}A = 0 \ \text{ if } \ p > 0, \quad E^0_{0,*}A = E^0_{0,0}A = R, \quad \text{and} \quad E^0_{-1,*}A = QA.$$

If A is an associative quasi bialgebra with split product filtration, then E^0A is a primitive bialgebra since the elements of $E^0_{-1,*}A$ generate E^0A and are evidently primitive, and this implies coassociativity.

Definition 2.10. Let C be a unital coalgebra. Define the coproduct filtration $\{F_pC\}$ by $F_pC = 0$ if $p < 0$, $F_0C = R$, and $F_pC = \ker \bar{\psi}_p$ if $p > 0$, where $\bar{\psi}_p$ is the composite

$$IC \subset C \xrightarrow{\psi_p} C \otimes \ldots \otimes C \longrightarrow JC \otimes \ldots \otimes JC, \quad p \ \text{ factors.}$$

Observe that

$$E^0_{p,*}C = 0 \ \text{ if } \ p < 0, \quad E^0_{0,*}C = E^0_{0,0}C = R, \quad \text{and} \quad E^0_{1,*}C = PC.$$

If C is a coassociative quasi bialgebra with split coproduct filtration, then E^0C is a coprimitive bialgebra since the elements of $E^0_{-1,*}C$ are evidently indecomposable and include all the primitives; Lemma 1.1 below implies that E^0C is associative.

3. Antipodes and Hopf algebras

For a monoid G, the monoid ring $R[G]$ is a bialgebra with product, coproduct, unit and counit induced by the product, diagonal, identity element, and trivial function $G \longrightarrow \{pt\}$. If G is a group, its inverse function induces an antipode on $R[G]$, in the sense of the following definition.

Definition 3.1. An antipode χ on a bialgebra A is a map $\chi : A \to A$ of R-modules such that the following diagrams commute.

$$\begin{tikzcd}
A \otimes A \arrow[rr, "\mathrm{id} \otimes \chi"] & & A \otimes A \arrow[d, "\phi"] \\
A \arrow[u, "\psi"] \arrow[r, "\varepsilon"'] & R \arrow[r, "\eta"'] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
A \otimes A \arrow[rr, "\chi \otimes \mathrm{id}"] & & A \otimes A \arrow[d, "\phi"] \\
A \arrow[u, "\psi"] \arrow[r, "\varepsilon"'] & R \arrow[r, "\eta"'] & A
\end{tikzcd}$$

A Hopf algebra is a bialgebra with a given antipode.

If A and B have antipodes χ, then $A \otimes B$ has the antipode $\chi \otimes \chi$.

Remark 3.2. The original definition of an antipode in Milnor and Moore [**?**] required only one of these two diagrams to commute, since in the cases of interest in algebraic topology, if one of them commutes, then so does the other. Actually, in [**?**] and most of the topological literature, the term "conjugate" is used instead of "antipode". Historically, the concept of Hopf algebra originated in algebraic topology, where the term "Hopf algebra" was used for what we are calling a bialgebra. The term bialgebra was introduced later and is still rarely used in topology. In fact, as we shall see in §3, the bialgebras that usually appear in algebraic topology automatically have antipodes, so that it is reasonable to ignore the distinction, and we do so where no confusion can arise. We have followed the algebraic literature in using the name antipode and distinguishing between bialgebras and Hopf algebras because of the more recent interest in Hopf algebras of a kind that do not seem to appear in algebraic topology, such as quantum groups.

Remark 3.3. In general, the existence and properties of antipodes is a subtle question. For example, χ can exist but not satisfy $\chi^2 = \mathrm{id}$. The order of an antipode χ is defined to be the minimum n such that $\chi^n = \mathrm{id}$. It can be any even number or can even be infinite [**?**, p. 89].

In the cocommutative case, the concepts of bialgebra and Hopf algebra can be given a pleasant conceptual form. It is a standard and easy observation that the tensor product is the categorical coproduct in the category of commutative algebras. The units of A and B induce maps of algebras $i\colon A \longrightarrow A\otimes B \longleftarrow B\colon j$, and for any algebra maps $f\colon A \longrightarrow C \longleftarrow B\colon g$, the composite of $f\otimes g$ and the product on C gives the unique map of algebras $h\colon A\otimes B \longrightarrow C$ such that $h\circ i = f$ and $h\circ j = g$. We are interested in the dual observation. Recall that, in any category with products, we have the notion of a monoid, namely an object with an associative and unital product, and of a group, namely a monoid with an antipode. The following result is immediate from the definitions.

Proposition 3.4. *The tensor product is the categorical product in the category $\mathscr{C}$ of commutative coalgebras. A cocommutative bialgebra is a monoid in $\mathscr{C}$, and a cocommutative Hopf algebra is a group in $\mathscr{C}$.*

There is another conceptual way of thinking about antipodes. It is based on the following construction.

Construction 3.5. Let C be a coalgebra and A be an algebra. Then $\mathrm{Hom}(C, A)$ is an algebra, called a convolution algebra. Its unit element is the composite $C \xrightarrow{\varepsilon} R \xrightarrow{\eta} A$ and its product is the composite

$$*\colon \mathrm{Hom}(C,A)\otimes \mathrm{Hom}(C,A) \xrightarrow{\alpha} \mathrm{Hom}(C\otimes C, A\otimes A) \xrightarrow{\mathrm{Hom}(\psi,\phi)} \mathrm{Hom}(C,A).$$

If C is unital with unit η and A is augmented with augmentation ε, then the set $G(C,A)$ of maps of R-modules $f\colon C \longrightarrow A$ such that $f\eta = \eta$ and $\varepsilon f = \varepsilon$ is a submonoid of $\mathrm{Hom}(C,A)$ under the convolution product $*$.

Remark 3.6. Visibly, when A is a bialgebra, an antipode is a (two-sided) inverse to the identity map $A \longrightarrow A$ in the monoid $G(A,A)$. Therefore χ is unique if it exists. This remark is one reason to prefer the two-sided rather than one-sided definition of an antipode.

Clearly, a sensible way to prove that a bialgebra A is a Hopf algebra is to prove more generally that $G(A,A)$ is a group. We return to this point in §3, where we give an easy general result of this form that applies to the examples of interest in algebraic topology.

4. Modules, comodules, and related concepts

There are many further basic pairs of dual algebraic definitions.

Definition 4.1. Let (A, ϕ, η) be an algebra. A left A-module (N, ξ) is an R-module N and action $\xi : A \otimes N \to N$ such that the following diagrams commute.

$$\begin{tikzcd}
A \otimes A \otimes N \arrow[r, "\mathrm{id} \otimes \xi"] \arrow[d, "\phi \otimes \mathrm{id}"'] & A \otimes N \arrow[d, "\xi"] \\
A \otimes N \arrow[r, "\xi"'] & N
\end{tikzcd}$$

and

$$\begin{tikzcd}
A \otimes N \arrow[d, "\xi"'] & R \otimes N \arrow[l, "\eta \otimes \mathrm{id}"'] \arrow[dl, equal] \\
N &
\end{tikzcd}$$

For an R-module N, $(A \otimes N, \phi \otimes \mathrm{id})$ is an A-module and is said to be an extended A-module. For an A-module (N, ξ), ξ is a morphism of A-modules. With kernels and cokernels defined degreewise, the category of left A-modules is abelian. There is an analogous abelian category of right A-modules. For a right A-module (M, λ) and left A-module (N, ξ), the tensor product $M \otimes_A N$, which of course is just an R-module, can be described as the cokernel of

$$\lambda \otimes \mathrm{id} - \mathrm{id} \otimes \xi : M \otimes A \otimes N \to M \otimes N;$$

$\otimes_A$ is a right exact functor of M and of N.

Definition 4.2. Given an augmentation $\varepsilon : A \to R$ of A, regard R as a (left and right) A-module via ε and define

$$Q_A N = R \otimes_A N = N / IA \cdot N;$$

$Q_A N$ is called the module of A-indecomposable elements of N and is abbreviated QN when there is no danger of confusion. Observe that $Q_A(IA) = QA$.

Definition 4.3. Let (C, ψ, ε) be a coalgebra. A left C-comodule (N, ν) is an R-module N and coaction $\nu : N \to C \otimes N$ such that the following diagrams commute.

$$\begin{tikzcd}
N \arrow[r, "\nu"] \arrow[d, "\nu"'] & C \otimes N \arrow[d, "\psi \otimes \mathrm{id}"] \\
C \otimes N \arrow[r, "\mathrm{id} \otimes \nu"'] & C \otimes C \otimes N
\end{tikzcd}$$

and

$$\begin{tikzcd}
N \arrow[d, "\nu"'] \arrow[dr, equal] & \\
C \otimes N \arrow[r, "\varepsilon \otimes \mathrm{id}"'] & R \otimes N
\end{tikzcd}$$

For an R-module N, $(C \otimes N, \psi \otimes \mathrm{id})$ is a C-comodule, said to be a coextended C-comodule. For a C-comodule (N, ν), ν is a morphism of C-comodules. Since $\otimes$ is right but not left exact, the category of left C-comodules does not admit kernels in general; it is abelian if C is a flat R-module. There is an analogous category of right C-comodules. For a right C-comodule (M, μ) and a left C-comodule (N, ν), define the cotensor product $M \square_C N$ to be the kernel of

$$\mu \otimes \mathrm{id} - \mathrm{id} \otimes \nu : M \otimes N \to M \otimes C \otimes N.$$

The functor $\square$ is left exact with respect to sequences of left or right C-comodules which are split exact as sequences of R-modules (in the sense that the kernel at each position is a direct summand).

Definition 4.4. Given a unit $\eta \colon R \to C$, regard R as a (left and right) C-comodule via η and define

$$P_C N = R \square_C N = \{ n | \nu(n) = 1 \otimes n \};$$

$P_C N$ is called the module of C-primitive elements of N and is abbreviated PN when there is no danger of confusion. Observe that $P_C(JC) = PC$.

The following definition is fundamental. For a general algebra A, the tensor product (over R) of A-modules is an $A \otimes A$-module, but for bialgebras we can internalize this structure by pullback along ψ.

Definition 4.5. Let $(A, \phi, \psi, \eta, \varepsilon)$ be a bialgebra. For left A-modules (N, ξ) and (N', ξ'), the following composite defines a left A-module structure on $N \otimes N'$.

$$A \otimes N \otimes N' \xrightarrow{(\mathrm{id} \otimes \gamma \otimes \mathrm{id})(\psi \otimes \mathrm{id})} A \otimes N \otimes A \otimes N' \xrightarrow{\xi \otimes \xi'} N \otimes N'$$

An A-structure (module, coalgebra, algebra, bialgebra, Hopf algebra, etc) is an A-module and a structure of the specified type such that all the maps which define the structure are morphisms of A-modules. Dually, for left A-comodules (N, ν) and (N', ν'), the following composite defines a left A-comodule structure on $N \otimes N'$.

$$N \otimes N' \xrightarrow{\nu \otimes \nu'} A \otimes N \otimes A \otimes N' \xrightarrow{(\phi \otimes \mathrm{id})(\mathrm{id} \otimes \gamma \otimes \mathrm{id})} A \otimes N \otimes N'$$

The dual notion of an A-comodule and a structure whose structural maps are morphisms of A-comodules will be referred to as an A-comodule structure.

Lemma 4.6. *Let A be an algebra and N be an R-module, both projective of finite type.*

(i) (N, ξ) is a left A-module if and only if (N^*, ξ^*) is a left A^*-comodule and then, if QN is also projective of finite type, $(QN)^* = P(N^*)$.

(ii) If A is a bialgebra, then N is a left A-structure if and only if N^* is a left A^*-comodule structure of the dual type.

Lemma 4.7. *Let A be a bialgebra and C be a left A-coalgebra. Then $Q_A C$ admits a unique structure of coalgebra such that the natural epimorphism $\pi : C \to Q_A C$ is a morphism of coalgebras.*

Proof. The augmentation of $Q_A C = R \otimes_A C$ is the map

$$\mathrm{id} \otimes \varepsilon \colon R \otimes_A C \to R \otimes_A R = R$$

and the coproduct is the composite of

$$\mathrm{id} \otimes \psi : R \otimes_A C \to R \otimes_A (C \otimes C)$$

and the natural map $R \otimes_A (C \otimes C) \to (R \otimes_A C) \otimes (R \otimes_A C)$. □

Note that any bialgebra C which contains A as a sub bialgebra is certainly a left A-coalgebra.

Lemma 4.8. *Let A be a bialgebra and B be a left A-comodule algebra. Then $P_A B$ admits a unique structure of algebra such that the natural monomorphism $\iota : P_A B \to B$ is a morphism of algebras.*

Definition 4.9. A morphism $f : A \to B$ of augmented algebras is said to be normal if the images of the composites

$$IA \otimes B \xrightarrow{f \otimes \mathrm{id}} B \otimes B \xrightarrow{\phi} B \qquad \text{and} \qquad B \otimes IA \xrightarrow{\mathrm{id} \otimes f} B \otimes B \xrightarrow{\phi} B$$

are equal and if the quotient map $\pi : B \to B//f$ is a split epimorphism, where $B//f$ is defined to be the R-module

$$Q_A B = R \otimes_A B = B/IA \cdot B = B/B \cdot IA = B \otimes_A R.$$

When f is an inclusion, $B//f$ is generally written $B//A$. Clearly $B//f$ admits a unique structure of augmented algebra such that π is a morphism of augmented algebras, and the following is an exact sequence of R-modules.

$$\begin{tikzcd} QA \arrow[r, "Qf"] & QB \arrow[r, "Q\pi"] & Q(B//f) \arrow[r] & 0 \end{tikzcd}$$

Definition 4.10. A morphism $g : B \to C$ of unital coalgebras is said to be conormal if the kernels of the composites

$$\begin{tikzcd} B \arrow[r, "\psi"] & B \otimes B \arrow[r, "g\otimes \mathrm{id}"] & JC \otimes B \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} B \arrow[r, "\psi"] & B \otimes B \arrow[r, "\mathrm{id}\otimes g"] & B \otimes JC \end{tikzcd}$$

are equal and if the inclusion $\iota : B\backslash\backslash g \to B$ is a split monomorphism, where $B\backslash\backslash g$ is defined to be the R-module

$$P_C B = R\Box_C B = \ker(g\otimes \mathrm{id})\psi = \ker(\mathrm{id}\otimes g)\psi = B\Box_C R.$$

When g is an epimorphism, $B\backslash\backslash g$ is generally written $B\backslash\backslash C$. Clearly $B\backslash\backslash g$ admits a unique structure of unital coalgebra such that ι is a morphism of unital coalgebras, and the following is an exact sequence of R-modules

$$\begin{tikzcd} 0 \arrow[r] & P(B\backslash\backslash g) \arrow[r, "P\iota"] & PB \arrow[r, "Pg"] & PC. \end{tikzcd}$$

When R is a field, any morphism of commutative augmented algebras is normal and any morphism of cocommutative unital coalgebras is conormal.

Remark 4.11. Let $f : A \to B$ be a morphism of bialgebras. If f is normal, then $B//f$ is a quotient bialgebra of B by Lemma 4.7. If f is conormal, then $A\backslash\backslash f$ is a sub bialgebra of A by Lemma 4.8. The first assertion generalizes. A two-sided ideal $J \subset IB$ is said to be a Hopf ideal if

$$\psi(J) \subset B\otimes J + J \otimes B,$$

and then B/J (if flat) is a quotient bialgebra of B.

We emphasize that the previous few definitions and results work equally well if bialgebras are replaced by Hopf algebras everywhere.

CHAPTER 2

Connected and component Hopf algebras

An R-module A such that $A_i = 0$ for $i < 0$ (as we have tacitly assumed throughout) and $A_0 = R$ is said to be connected. Note that a connected algebra admits a unique augmentation and a connected coalgebra admits a unique unit. We shall see in §3 that a connected bialgebra always admits a unique antipode. Except in §3, we therefore follow the literature of algebraic topology and only use the term Hopf algebra in this chapter, since there is no real difference between the notions when A is connected. Connected structures arise ubiquitously in topology and have many special properties. For example, the homology of a connected homotopy associative H-space X is a connected Hopf algbra. The homology of non-connected but grouplike ($\pi_0(X)$ is a group) homotopy associative H-spaces leads to the more general notion of a component Hopf algebra. When concentrated in degree zero, these are just the classical group algebras $R[G]$. These too have unique antipodes.

We prove basic theorems on the splitting of connected algebras and coalgebras over a connected Hopf algebra in §2, and we prove the self-duality of free commutative and cocommutative connected Hopf algebras on a single generator in §4. To illustrate the power of these beautiful but elementary algebraic results, we show how they can be used to prove Thom's calculation of unoriented cobordism and Bott's periodicity theorem for BU in §5 and §6.

1. Connected algebras, coalgebras, and Hopf algebras

We here prove various special properties that hold in the connected case but do not hold in general. However, they generally do apply to bigraded objects that are connected to the eyes of one of the gradings, and such structures can arise from filtrations of objects that are not connected.

LEMMA 1.1. *Let A be a connected coprimitive quasi Hopf algebra. Then A is associative and commutative. If the characteristic of R is a prime p, then the p^{th} power operation ξ (defined only on even degree elements of A if $p > 2$) is identically zero on IA.*

PROOF. Write $a(x,y,z) = x(yz) - (xy)z$ and $[x,y] = xy - (-1)^{\deg x \deg y} yx$. If x, y, and z are primitive elements of IA, then $a(x,y,z)$, $[x,y]$, and $\xi(x)$ are also primitive by direct calculation from Lemma 2.6 and the fact that the coproduct is a map of algebras. Since these elements obviously map to zero in QA, they must be zero. Now proceed by induction on $q = \deg x$, for fixed q by induction on $r = \deg y$, and for fixed q and r by induction on $s = \deg z$. By calculation from the induction hypothesis at each stage, we find that $a(x,y,z)$, $[x,y]$, and $\xi(x)$ are primitive and therefore zero. Here we prove commutativity before handling p^{th} powers so as to ensure that $(x+y)^p = x^p + y^p$. □

A Prüfer ring is an integral domain all of whose ideals are flat. A Noetherian Prüfer ring is a Dedekind ring.

Lemma 1.2. *A connected Hopf algebra A over a Prufer ring R is the colimit of its sub Hopf algebras of finite type.*

Proof. Since R is Prufer, every submodule of the flat R-module A is flat. Any element of A lies in a finitely generated sub algebra B, and B is clearly of finite type. An inductive argument based on the form of $\psi(x)$ given in Lemma 2.6 shows that the smallest sub Hopf algebra of A which contains B is also finitely generated. □

Proposition 1.3. *If $f : A \to B$ is a morphism of augmented algebras, where B is connected, then f is an epimorphism if and only if Qf is an epimorphism.*

Proof. Certainly Qf is an epimorphism if f is. Suppose that Qf is an epimorphism. By application of the five lemma to the commutative diagram with exact rows

$$\begin{tikzcd}
IA \otimes IA \arrow[r] \arrow[d, "f\otimes f"'] & IA \arrow[r] \arrow[d, "f"] & QA \arrow[r] \arrow[d, "Qf"] & 0 \\
IB \otimes IB \arrow[r] & IB \arrow[r] & QB \arrow[r] & 0
\end{tikzcd}$$

we see by induction on n that f is an epimorphism in degree n for all n since f is trivially an epimorphism in degree 0 by the connectivity of B. □

Proposition 1.4. *If $f : A \to B$ is a morphism of R-flat unital coalgebras, where A is connected, then f is a monomorphism if and only if $Pf : PA \to PB$ is a monomorphism.*

Proof. The argument is dual to that just given. The flatness hypothesis ensures that $f \otimes f : JA \otimes JA \to JB \otimes JB$ is a monomorphism in degree n if f is a monomorphism in degrees less than n. □

The following result is a version of "Nakayama's lemma". It and its dual are used constantly in algebraic topology.

Lemma 1.5. *If A is a connected algebra and N is a left A-module, then $N = 0$ if and only if $QN = 0$.*

Proof. Clearly $QN = 0$ if and only if $IA \otimes N \to N$ is an epimorphism, and this implies that N is zero by induction on degrees. □

Lemma 1.6. *If A is a connected algebra and $f : N \to N'$ is a morphism of left A-modules, then f is an epimorphism if and only if $Qf : QN \to QN'$ is an epimorphism.*

Proof. The functor Q is right exact, hence $Q\,\mathrm{coker}\, f = 0$ and therefore $\mathrm{coker}\, f = 0$ if Qf is an epimorphism. □

The duals of the previous two results read as follows.

Lemma 1.7. *If C is a connected coalgebra and N is a left C-comodule, then $N = 0$ if and only if $PN = 0$.*

Lemma 1.8. *If C is an R-flat connected coalgehra and $f : N \to N'$ is a morphism of left C-comodules, then f is a monomorphism if and only if Pf is a monomorphism.*

2. Splitting theorems

We here prove the basic results of Milnor and Moore on tensor product decompositions of connected Hopf algebras. These play a key role in many calculations, for example in the calculation of the cobordism rings of manifolds.

Theorem 2.1. *Let A be a connected Hopf alqebra and B be a connected left A-coalgebra. Write $QB = Q_AB$ and assume that the quotient map $\pi : B \to QB$ is a split epimorphism. Define $\iota : A \to B$ by $\iota(a) = a\eta(1)$ and assume that $\iota \otimes \mathrm{id} : A \otimes QB \to B \otimes QB$ is a monomorphism. Then there is an isomorphism $f : B \to A \otimes QB$ which is a map of both left A-modules and right QB-comodules.*

Proof. Since π is a split epimorphism, we can choose a map of R-modules $\sigma : QB \to B$ such that $\pi\sigma = \mathrm{id}$. Let $g : A \otimes QB \to B$ be the induced map of left A-modules. Since $Qg : QB = Q(A \otimes QB) \to QB$ is the identity, g is an epimorphism by Lemma 1.6. We have the following composite of morphisms of A-modules.

$$h : A \otimes QB \xrightarrow{g} B \xrightarrow{\psi} B \otimes B \xrightarrow{\mathrm{id} \otimes \pi} B \otimes QB$$

Here A acts through $\varepsilon : A \to R$ on QB and acts diagonally on the tensor products. We claim that h is a monomorphism, so that g is a monomorphism and therefore an isomorphism. Filter $A \otimes QB$ by the degrees of elements of QB,

$$F_p(A \otimes QB) = \sum_{i \le p} A \otimes Q_iB,$$

The associated bigraded module of $A \otimes QB$ satisfies

$$E^0_{p,q}(A \otimes QB) = A_q \otimes Q_pB.$$

Filter $B \otimes QB$ similarly. Since h is a morphism of A-modules and is clearly filtration-preserving when restricted to QB, it is filtration-preserving. Since $\pi(an) = 0$ unless $\deg(a) = 0$, we see that $E^0h = \iota \otimes \mathrm{id}$ and thus E^0h is a monomorphism by hypothesis. By Proposition 1.1, it follows that h is a monomorphism, as claimed. Now observe that $g(a \otimes \eta(1)) = \iota(a)$ for $a \in A$ and thus $(\mathrm{id} \otimes \varepsilon)g^{-1}\iota = \mathrm{id} : A \to A$, $\varepsilon : QB \to R$. Define f to be the composite

$$B \xrightarrow{\psi} B \otimes B \xrightarrow{\mathrm{id} \otimes \pi} B \otimes QB \xrightarrow{g^{-1} \otimes \mathrm{id}} A \otimes QB \otimes QB \xrightarrow{\mathrm{id} \otimes \varepsilon \otimes \mathrm{id}} A \otimes QB$$

Clearly f is a morphism of left A-modules and right QB-comodules. Recall the filtration on $A \otimes QB$. Inspection shows that $fg : A \otimes QB \to A \otimes QB$ is filtration-preserving and that

$$E^0(fg) = (\mathrm{id} \otimes \varepsilon)g^{-1}\iota \otimes \pi\sigma = \mathrm{id}\,.$$

Therefore, by Proposition 1.1, fg and thus also f is an isomorphism. □

Note that, in the hypotheses, $\iota \otimes \mathrm{id}$ will be a monomorphism if ι is a monomorphism and QB is flat. Since a direct summand of a flat module is flat, the assumption on π implies that QB is flat if B is flat. Of course, when R is a field, as is the case in most applications, the only assumption is that $\iota : A \to B$ be a monomorphism.

The dual result reads as follows. Recall that we require Hopf algebras to be R-flat.

Theorem 2.2. *Let C be a connected Hopf algebra and B be a connected left C-comodule algebra. Write $PB = P_C B$ and assume that the inclusion $\iota : PB \to B$ is a split monomorphism. Define $\pi : B \to C$ to be the composite of the coaction $\nu : B \to C \otimes B$ and $\mathrm{id} \otimes \varepsilon : C \otimes B \to C$ and assume that $\pi \otimes \mathrm{id} : B \otimes PB \to C \otimes PB$ is an epimorphism. Then there is an isomorphism $g : C \otimes PB \to B$ which is a map of both left C-comodules and right PB-modules.*

When R is a field, the only assumption is that $\pi : B \to C$ be an epimorphism.

These results are frequently applied to morphisms of Hopf algebras. Recall Definitions 4.9 and 4.10.

Theorem 2.3. *Let $\iota : A \to B$ and $\pi : B \to C$ be morphisms of connected Hopf algebras. The following are equivalent.*

(i) ι is a normal monomorphism, $C = B//A$, and π is the quotient map.

(ii) π is a conormal epimorphism, $A = B\backslash\backslash C$, and ι is the inclusion.

(iii) There is an isomorphism $f : A \otimes C \to B$ of left A-modules and right C-comodules and an isomorphism $g : C \otimes A \to B$ of right A-modules and left C-comodules.

When (i)–(iii) hold,

$$f(\mathrm{id} \otimes \eta) = \iota = g(\eta \otimes \mathrm{id}), \quad (\varepsilon \otimes \mathrm{id})f^{-1} = \pi = (\mathrm{id} \otimes \varepsilon)g^{-1},$$

and the following is a commutative diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & PA \arrow[r, "P\iota"] \arrow[d, "\nu"'] & PB \arrow[r, "P\pi"] \arrow[d, "\nu"] & PC \arrow[d, "\nu"] & \\
& QA \arrow[r, "Q\iota"'] & QB \arrow[r, "Q\pi"'] & QC \arrow[r] & 0
\end{tikzcd}$$

Proof. Clearly (i) implies (iii) by Theorem 2.1 and symmetry while (ii) implies (iii) by Theorem 2.2 and symmetry. When (iii) holds, the descriptions of ι and π in terms of f and g follow from the module and comodule morphism properties of f and g, and (i) and (ii) follow by inspection. The diagram is obvious. □

Corollary 2.4. *Let $A \to B$ and $B \to C$ be normal monomorphisms of connected Hopf algebras. Then $B \to C$ induces a normal monomorphism of connected Hopf algebras $B//A \to C//A$, and $(C//A)//(B//A)$ is isomorphic to $C//B$.*

Proof. $C \cong B \otimes C//B$, hence $C//A \cong B//A \otimes C//B$. and the conclusions follow. □

Corollary 2.5. *Let $A \to B$ and $B \to C$ be conormal epimorphisms of connected Hopf algebras. Then $A \to B$ induces a conormal epimorphism of connected Hopf algebras $A\backslash\backslash C \to B\backslash\backslash C$, and $(A\backslash\backslash C)\backslash\backslash(B\backslash\backslash C)$ is isomorphic to $A\backslash\backslash B$.*

3. Component coalgebras and the existence of antipodes

To prove the existence and develop the properties of χ on a bialgebra A, we need to make some hypothesis. However, the usual hypothesis in algebraic topology, connectivity, is too restrictive for many applications. We give a more general hypothesis, but still geared towards the applications in algebraic topology.

Definition 3.1. We define grouplike algebras and component coalgebras.

(i) An augmented algebra A is said to be grouplike if the set $\varepsilon^{-1}(1)$ of degree 0 elements is a group under the product of A.

(ii) Let C be a coalgebra such that C_0 is R-free and define

$$\pi C = \{g | \psi(g) = g \otimes g \text{ and } g \neq 0\} \subset C_0.$$

For $g \in \pi C$, $g = \varepsilon(g)g$ by the counit property and thus $\varepsilon(g) = 1$ since C_0 is assumed to be R-free. Define the component C_g of g by letting $C_g = Rg \oplus \bar{C}_g$, where the R-module $\bar{C}_g$ of positive degree elements of C_g is

$$\{x | \psi(x) = x \otimes g + \sum x' \otimes x'' + g \otimes x, \quad \deg x' > 0 \quad \text{and} \quad \deg x'' > 0\}.$$

(iii) Say that C is a component coalgebra if C_0 is R-free, each C_g is a sub coalgebra of C, and C is the direct sum of the C_g.

If C is unital then it has a privileged component, namely C_1. Note that primitivity becomes a less general notion in component coalgebras than intuition might suggest: elements x with $\psi(x) = x \otimes g + g \otimes x$, $g \neq 1$, are not primitive according to Definition 2.5.

If X is a based space, then $H_*(X; R)$, if R-flat, is a unital component coalgebra. Similarly, $H_*(\Omega X; R)$, if R-flat, is a grouplike component Hopf algebra; it is connected if and only if X is simply connected.

Now recall Construction 3.5. We implement the idea at the end of §3.

Lemma 3.2. *If C is a unital component coalgebra and A is a grouplike augmented algebra, then $G(C, A)$ is a group under the convolution product $*$.*

Proof. Let $f \in G(C, A)$. We must construct f^{-1}. Define $f^{-1}(g) = f(g)^{-1}$ for $g \in \pi C$ and extend f^{-1} to all of C_0 by R-linearity. Proceeding by induction on degrees, define $f^{-1}(x)$ for $x \in \bar{C}_g$ by

$$f^{-1}(x) = -f(g)^{-1} f(x) f(g)^{-1} - \sum f(g)^{-1} f(x') f^{-1}(x''),$$

where $\psi(x) = x \otimes g + \sum x' \otimes x'' + g \otimes x$, $\deg x > 0$ and $\deg x'' > 0$. Extend f^{-1} to C by R-linearity. Then $f * f^{-1} = \eta\varepsilon$ by direct inductive calculation. Of course, since every f has a right inverse, $f^{-1} * f = \eta\varepsilon$ follows formally. □

Proposition 3.3. *Let A be a grouplike component bialgebra. Then A admits a (unique) antipode χ, so that*

$$\phi(\mathrm{id} \otimes \chi)\psi = \eta\varepsilon = \phi(\chi \otimes \mathrm{id})\psi.$$

Further, the following two diagrams are commutative,

$$\begin{tikzcd} A \arrow[r, "\psi"] \arrow[d, "\chi"'] & A \otimes A \arrow[r, "\gamma"] & A \otimes A \arrow[d, "\chi\otimes\chi"] \\ A \arrow[rr, "\psi"'] & & A \otimes A \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \otimes A \arrow[r, "\gamma"] \arrow[d, "\chi\otimes\chi"'] & A \otimes A \arrow[r, "\phi"] & A \arrow[d, "\chi"] \\ A \otimes A \arrow[rr, "\phi"'] & & A \end{tikzcd}$$

Moreover, if A is either commutative or cocommutative, then $\chi^2 \equiv \chi \circ \chi = \mathrm{id}$.

PROOF. The first statement is immediate from Lemma 3.2. For the first diagram, we claim that both $\psi\chi$ and $(\chi\otimes\chi)\gamma\psi$ are the inverse of $\psi : A \to A\otimes A$ in the group $G(A, A\otimes A)$. Indeed, we have

$$\psi * \psi\chi = (\phi\otimes\phi)(\mathrm{id}\otimes\gamma\otimes\mathrm{id})(\psi\otimes\psi\chi)\psi = \psi\phi(\mathrm{id}\otimes\chi)\psi = \psi\eta\varepsilon = \eta\varepsilon$$

by the very definition of a bialgebra. Since χ is natural and $\gamma : A\otimes A \to A\otimes A$ is an automorphism of Hopf algebras, $(\chi\otimes\chi)\gamma = \gamma(\chi\otimes\chi)$. Thus

$$\begin{aligned}
\psi * (\chi\otimes\chi)\gamma\psi &= (\phi\otimes\phi)(\mathrm{id}\otimes\gamma\otimes\mathrm{id})(\psi\otimes\gamma(\chi\otimes\chi)\psi)\psi \\
&= (\phi\otimes\phi)(\mathrm{id}\otimes\gamma\otimes\mathrm{id})(\mathrm{id}\otimes\mathrm{id}\otimes\gamma)(\mathrm{id}\otimes\mathrm{id}\otimes\chi\otimes\chi)(\psi\otimes\psi)\psi \\
&= (\phi\otimes\mathrm{id})(\mathrm{id}\otimes\gamma)(\mathrm{id}\otimes\phi\otimes\mathrm{id})(\mathrm{id}\otimes\mathrm{id}\otimes\chi\otimes\chi)(\mathrm{id}\otimes\psi\otimes\mathrm{id})(\psi\otimes\mathrm{id})\psi \\
&= (\phi\otimes\mathrm{id})(\mathrm{id}\otimes\gamma)(\mathrm{id}\otimes\eta\varepsilon\otimes\chi)(\psi\otimes\mathrm{id})\psi \\
&= (\phi\otimes\mathrm{id})(\mathrm{id}\otimes\chi\otimes\eta\varepsilon)(\psi\otimes\mathrm{id})\psi \\
&= (\eta\varepsilon\otimes\eta\varepsilon)\psi = \eta\varepsilon.
\end{aligned}$$

The proof of the second diagram is dual. Finally, to show that $\chi^2 = \mathrm{id}$, it suffices to show that χ^2 is the inverse of χ in the group $G(A, A)$. If A commutative, the second diagram in the statement gives

$$\chi^2 * \chi = \phi(\chi^2 * \chi)\psi = \phi(\chi\otimes\chi)(\chi\otimes\mathrm{id})\psi = \chi\phi\gamma(\chi\otimes\mathrm{id})\psi = \chi\eta\varepsilon = \eta\varepsilon.$$

The proof that $\chi^2 = \mathrm{id}$ when A is cocommutative is dual. □

Note that the second diagram of the statement asserts that χ is a graded involution. In the connected case, the result specializes to give the following simpler formula for the antipode.

$$\chi(x) = -x - \sum x'\chi(x'') \tag{3.4}$$

if $\deg x > 0$ and $\psi(x) = x\otimes 1 + \sum x'\otimes x'' + 1\otimes x$, $\deg x' > 0$ and $\deg x'' > 0$.

4. Self-dual Hopf algebras

The homology Hopf algebras $H_*(BU;\mathbb{Z})$ and $H_*(BO;\mathbb{F}_2)$ enjoy a very special property: they are self-dual, so that they are isomorphic to the cohomology Hopf algebras $H^*(BU;\mathbb{Z})$ and $H^*(BO;\mathbb{F}_2)$. The proof of this basic result is purely algebraic and explicitly determines the homology Hopf algebras from the cohomology Hopf algebras (or vice versa if one calculates in the opposite order). We assume that the reader knows that the cohomology Hopf algebras are given by

$$H^*(BU;\mathbb{Z}) = P\{c_i \mid i \geq 1\} \quad \text{with} \quad \psi(c_n) = \sum_{i+j=n} c_i\otimes c_j \tag{4.1}$$

and

$$H^*(BO;\mathbb{F}_2) = P\{w_i \mid i \geq 1\} \quad \text{with} \quad \psi(w_n) = \sum_{i+j=n} w_i\otimes w_j\,. \tag{4.2}$$

The calculations of $H^*(BU(n);\mathbb{Z})$ and $H^*(BO(n);\mathbb{F}_2)$ are summarized in [**?**, pp 187, 195], and passage to colimits over n gives the stated conclusions. Thus determination of the homology algebras is a purely algebraic problem in dualization.[1]

Recall that the dual coalgebra of a polynomial algebra $P[x]$ over R is written $\Gamma[x]$; when $P[x]$ is regarded as a Hopf algebra with x primitive, $\Gamma[x]$ is called a divided polynomial Hopf algebra.

[1] We thank John Rognes, who texed this section from the first author's notes in 1996.

Clearly $H^*(BU(1);\mathbb{Z}) = P[c_1]$ and $H^*(BO(1);\mathbb{F}_2) = P[w_1]$ are quotient algebras of $H^*(BU;\mathbb{Z})$ and $H^*(BO;\mathbb{F}_2)$. Write $H_*(BU(1);\mathbb{Z}) = \Gamma[\gamma_1]$; it has basis $\{\gamma_i \mid i \geq 0\}$ and coproduct $\psi(\gamma_n) = \sum_{i+j=n} \gamma_i \otimes \gamma_j$, where $\gamma_0 = 1$ and γ_i is dual to c_1^i. Write $H_*(BO(1);\mathbb{F}_2) = \Gamma[\gamma_1]$ similarly. The inclusions $BU(1) \longrightarrow BU$ and $BO(1) \longrightarrow BO$ induce identifications of these homologies with sub coalgebras of $H_*(BU;\mathbb{Z})$ and $H_*(BO;\mathbb{F}_2)$, and we shall prove that these sub coalgebras freely generate the respective homology algebras.

Theorem 4.3. *$H_*(BU;\mathbb{Z}) = P\{\gamma_i \mid i \geq 1\}$, where $\gamma_i \in H_*(BU(1);\mathbb{Z})$ is dual to c_1^i. The basis $\{p_i\}$ for the primitive elements of $H_*(BU;\mathbb{Z})$ such that $\langle c_i, p_i\rangle = 1$ is specified inductively by*

$$p_1 = \gamma_1 \quad \textit{and} \quad p_i = (-1)^{i+1} i\gamma_i + \sum_{j=1}^{i-1} (-1)^{j+1}\gamma_j p_{i-j} \quad \textit{for } i > 0.$$

This recursion formula is generally ascribed to Newton, of course in a different but related context, although the following explicit evaluation was known even earlier (to Girard, in a 1629 paper).

Remark 4.4. An explicit formula for p_i is given by

$$p_i = \sum_E (-1)^{|E|+i} \frac{(|E|-1)!i}{e_1! \cdots e_r!} \gamma^E.$$

Here the sum is taken over all sequences $E = (e_1, \ldots, e_r)$ with $e_q \geq 0$ and $\sum qe_q = i$; $|E| = \sum e_q$ and $\gamma^E = \gamma_1^{e_1} \cdots \gamma_r^{e_r}$.

Theorem 4.5. *$H_*(BO;\mathbb{F}_2) = P\{\gamma_i \mid i \geq 1\}$, where $\gamma_i \in H_*(BO(1);\mathbb{F}_2)$ is dual to w_1^i. The nonzero primitive elements of $H_*(BO;\mathbb{F}_2)$ are specified inductively by*

$$p_1 = \gamma_1 \quad \textit{and} \quad p_i = i\gamma_i + \sum_{j=1}^{i-1} \gamma_j p_{i-j} \quad \textit{for } i > 0.$$

Comparison of these theorems to (4.1) and (4.2) shows that $H^*(BU;\mathbb{Z})$ and $H^*(BO;\mathbb{F}_2)$ are self–dual; that is, they are isomorphic as Hopf algebras to their own duals. Following Moore [**?**], we shall carry out the proofs by considering self–duality for certain general types of Hopf algebras.

We work in the category of connected free R-modules X of finite type, so that $X_i = 0$ for $i < 0$ and $X_0 = R$. Throughout the discussion, all algebras are to be commutative and all coalgebras are to be cocommutative. Thus all Hopf algebras are to be commutative and cocommutative.

Definition 4.6. We define some universal Hopf algebras.

(i) A universal enveloping Hopf algebra of a coalgebra C is a Hopf algebra LC together with a morphism $i\colon C \longrightarrow LC$ of coalgebras which is universal with respect to maps of coalgebras $f\colon C \longrightarrow B$, where B is a Hopf algebra. That is, any such f factors uniquely as $\tilde{f} \circ i$ for a morphism $\tilde{f}\colon LC \longrightarrow B$ of Hopf algebras.

(ii) A universal covering Hopf algebra of an algebra A is a Hopf algebra MA together with a morphism $p\colon MA \longrightarrow A$ of algebras which is universal with respect to maps of algebras $f\colon B \longrightarrow A$, where B is a Hopf algebra. That is, any such f factors uniquely as $p \circ \tilde{f}$ for a morphism $\tilde{f}\colon B \longrightarrow MA$ of Hopf algebras.

Lemma 4.7. *Universal Hopf algebras exist and are unique. That is,*

(i) any coalgebra C admits a universal enveloping Hopf algebra $i\colon C \longrightarrow LC$;
(ii) any algebra A admits a universal covering Hopf algebra $p\colon MA \longrightarrow A$.

Proof. Of course, uniqueness up to isomorphism follows from universality. For (i), we have $C = R \oplus JC$, where JC is the module of positive degree elements of C. As an algebra, we take $LC = A(JC)$, the free (graded) commutative algebra generated by JC. Let $i\colon C \longrightarrow LC$ be the natural inclusion $JC \longrightarrow LC$ in positive degrees and the identity map id of R in degree zero. If ψ is the coproduct of C, the coproduct of LC is defined to be the unique map of algebras $\psi\colon LC \longrightarrow LC \otimes LC$ that makes the following diagram commute:

$$\begin{tikzcd}
C \arrow[r, "\psi"] \arrow[d, "i"'] & C \otimes C \arrow[d, "i\otimes i"] \\
LC \arrow[r, "\psi"'] & LC \otimes LC.
\end{tikzcd}$$

That ψ defines a coalgebra and thus a Hopf algebra structure on LC and that $i\colon C \longrightarrow LC$ is universal follow directly from the universal property of LC as an algebra. For (ii), since all modules are taken to be free of finite type, $p\colon MA \longrightarrow A$ can be specified as $i^*\colon (L(A^*))^* \longrightarrow A^{**} = A$. □

Remark 4.8. Similar constructions may be obtained when we omit some or all of the commutativity hypotheses. We can define universal enveloping commutative Hopf algebras for arbitrary coalgebras and universal covering cocommutative Hopf algebras for arbitrary algebras. These will coincide with our present constructions under our hypotheses. The universal enveloping non–commutative Hopf algebra is of course a quite different construction.

We shall shortly require a pair of dual lemmas, for which we need some notations. For an R-module X, let X^n denote the n-fold tensor product of X with itself. With the usual sign $(-1)^{\deg x \deg y}$ inserted when x is permuted past y, the symmetric group Σ_n acts on X^n. If X is an algebra or coalgebra, then so is X^n, and Σ_n acts as a group of automorphisms. Let Σ_n act trivially on LC and MA.

Lemma 4.9. *Let C be a coalgebra. For $n > 0$, define $\iota_n\colon C^n \longrightarrow LC$ to be the composite of $i^n\colon C^n \longrightarrow (LC)^n$ and the iterated product $\phi\colon (LC)^n \longrightarrow LC$. Then ι_n is a morphism of both Σ_n-modules and coalgebras. If $C_q = 0$ for $0 < q < m$, then ι_n is an epimorphism in degrees $q \leq mn$.*

Proof. The first statement is immediate from the definitions and the second statement follows from the fact that the image of ι_n is the span of the monomials in C of length at most n. □

Lemma 4.10. *Let A be an algebra. For $n > 0$, define $\pi_n\colon MA \longrightarrow A^n$ to be the composite of the iterated coproduct $\psi\colon MA \longrightarrow (MA)^n$ and $p^n\colon (MA)^n \longrightarrow A^n$. Then π_n is a morphism of both Σ_n-modules and algebras. If $A_q = 0$ for $0 < q < m$, then ι_n is a monomorphism in degrees $q \leq mn$.*

Proof. This follows by dualizing the previous lemma. □

Definition 4.11. Let X be positively graded R-module, so that $X_i = 0$ for $i \leq 0$. Define $LX = L(R \oplus X)$, where $R \oplus X$ is R in degree zero and has the trivial coalgebra structure, in which every element of X is primitive. Define $MX = M(R \oplus X)$, where $R \oplus X$ has the trivial algebra structure, in which the product of any two elements of X is zero. There is a natural morphism of Hopf algebras $\lambda\colon LMX \longrightarrow MLX$, which is defined in two equivalent ways. Indeed, consider the following diagram:

$$\begin{tikzcd}
LMX \arrow[rr, "\lambda"] \arrow[drr, "\mu" near end] & & MLX \arrow[d, "p"] \\
MX \arrow[u, "i"] \arrow[urr, "\nu" near start] \arrow[r, "p"'] & R \oplus X \arrow[r, "i"'] & LX.
\end{tikzcd}$$

Define μ to be $A(p)\colon A(JMX) \longrightarrow A(X)$, which is the unique morphism of algebras that extends $i \circ p$, and then obtain λ by the universal property of $p\colon MLX \longrightarrow LX$. Define ν to be the dual of $A(i^*)\colon A((JLX)^*) \longrightarrow A(X^*)$, so that ν is the unique morphism of coalgebras that covers $i \circ p$, and obtain λ by the universal property of $i\colon MX \longrightarrow LMX$. To see that the two definitions coincide, note that if λ is defined by the first property, then $\lambda \circ i = \nu$ by uniqueness and so λ also satisfies the second property.

Observe that $(R \oplus X)^*$ may be identified with $R \oplus X^*$. Since $MA = (L(A^*))^*$, it follows that

$$MX \equiv M(R \oplus X) = (L(R \oplus X^*))^* \equiv (L(X^*))^* .$$

In turn, with $A = L(X^*)$, this implies

$$ML(X^*) = MA = (L(A^*))^* = (L(L(X^*))^*)^* = (LMX)^* .$$

If X is R-free on a given basis, then the isomorphism $X \cong X^*$ determined by use of the dual basis induces an isomorphism of Hopf algebras

$$\beta\colon MLX \cong ML(X^*) = (LMX)^* .$$

When $\lambda\colon LMX \longrightarrow MLX$ is an isomorphism, it follows that LMX is self–dual. While λ is not always an isomorphism, it is so in the cases of greatest topological interest. We now regard $i\colon C \longrightarrow LC$ as an inclusion, omitting i from the notation. Write $\langle -, - \rangle$ for the usual pairing between a free R-module and its dual.

Theorem 4.12. *Let X be free on one generator x of degree m, where either m is even or R has characteristic two. Then $\lambda\colon LMX \longrightarrow MLX$ is an isomorphism. Moreover if*

$$c_i = \gamma_i(x) \in \Gamma[x] = MX \quad \textit{and} \quad \gamma_i = (\beta \circ \lambda)(c_i) \in (LMX)^*,$$

then γ_i is the basis element dual to c_1^i and the basis $\{p_i\}$ for the primitive elements of $(LMX)^*$ such that $\langle c_i, p_i \rangle = 1$ is specified inductively by

$$p_1 = \gamma_1 \quad \textit{and} \quad p_i = (-1)^{i+1} i \gamma_i + \sum_{j=1}^{i-1} (-1)^{j+1} \gamma_j p_{i-j} \quad \textit{for } i > 0.$$

Here $LMX = P\{c_i \mid i \geq 1\}$ with $\psi(c_n) = \sum_{i+j=n} c_i \otimes c_j$, where $c_0 = 1$. When $R = \mathbb{Z}$ and $m = 2$, LMX may be identified with $H^*(BU; \mathbb{Z})$ and $(LMX)^*$ may be identified with $H_*(BU; \mathbb{Z})$. Thus this result immediately implies Theorem 4.3.

Similarly, with $R = \mathbb{F}_2$ and $m = 1$, it implies Theorem 4.5. The rest of the section will be devoted to the proof.

PROOF. Note that $LX = P[x]$ and write $P[x]^n = P[x_1, \ldots, x_n]$, where $x_i = 1 \otimes \cdots \otimes 1 \otimes x \otimes 1 \otimes \cdots \otimes 1$ with x in the ith position. Let $\sigma_1, \ldots, \sigma_n$ be the elementary symmetric functions in the x_i. Consider $\pi_n \lambda \colon LMX \longrightarrow P[x]^n$, where $\pi_n = p^n \psi \colon MP[x] \longrightarrow P[x]^n$ is as specified in Lemma 4.10. From the diagram which defines λ, we see that $p\lambda \colon LMX \longrightarrow P[x]$ is given on generators by

$$p\lambda c_j = ipc_j = \begin{cases} x & \text{if } j = 1 \\ 0 & \text{if } j > 1. \end{cases}$$

Since λ is a morphism of Hopf algebras, it follows that

$$\pi_n \lambda c_j = p^n \psi \lambda c_j = p^n \lambda^n \psi c_j = (p\lambda)^n \Big(\sum_{i_1 + \cdots + i_n = j} c_{i_1} \otimes \cdots \otimes c_{i_n} \Big) = \begin{cases} \sigma_j & \text{if } j \leq n \\ 0 & \text{if } j > n. \end{cases}$$

Since $LMX = P[c_i]$, the map $\pi_n \lambda \colon P[c_i] \longrightarrow P[\sigma_1, \ldots, \sigma_n]$ is an isomorphism in degrees $q \leq mn$. By Lemma 4.10, π_n also takes values in $P[\sigma_1, \ldots, \sigma_n]$ and is a monomorphism in degrees $q \leq mn$. Therefore π_n and λ are both isomorphisms in degrees $q \leq mn$. Since n is arbitrary, this proves that λ is an isomorphism.

To see the duality properties of the γ_i, consider the map $\nu \colon \Gamma[x] \longrightarrow MP[x]$ in the diagram defining λ. Here ν is dual to $A(i^*) \colon A(J\Gamma[x^*]) \longrightarrow P[x^*]$, where x^* is the basis element of X^* dual to x, and i^* maps $\gamma_1(x^*)$ to x^* and annihilates $\gamma_i(x^*)$ for $i > 1$. Since $c_i = \gamma_i(x)$ is dual to $(x^*)^i$, $\nu(c_i)$ is dual to $\gamma_1(x^*)^i$ and thus $\eta\nu(c_i) = \gamma_i$ is dual to c_1^i.

Since the primitive elements of $(LMX)^*$ are dual to the indecomposable elements of LMX, they are free on one generator dual to c_i in each degree mi. We shall prove inductively that this generator is p_i, the case $i = 1$ having been handled above. Consider the term $\gamma_j p_{i-j}$, $1 \leq j \leq i - 1$, in the iterative expression for p_i. Let c^E be a monomial in the c_k, so that $E = (e_1, \ldots, e_r)$ and $c^E = c_1^{e_1} \cdots c_r^{e_r}$. Then

$$\langle c^E, \gamma_j p_{i-j} \rangle = \langle \psi c^E, \gamma_j \otimes p_{i-j} \rangle = \langle \psi c^E, (c_1^j)^* \otimes c_{i-j}^* \rangle$$

by the induction hypothesis and the calculation above. Consideration of the form of ψc^E shows that this is zero unless c^E is either $c_1^j c_{i-j}$ or $c_1^{j-1} c_{i-j+1}$, when it is one in all cases except the case $\langle c_1^i, \gamma_{i-1} p_1 \rangle = i$. It follows that $\langle c^E, p_i \rangle = 0$ except for the case $\langle c_i, p_i \rangle = 1$. An alternative argument is to verify inductively that each p_i is in fact primitive and then check that $\langle c_i, p_i \rangle = 1$. □

5. The homotopy groups of MO and other Thom spectra

In [**?**, Ch. 25], we explained Thom's classical computation of the real cobordism of smooth manifolds. In fact, the exposition there was something of a cheat. Knowing the splitting theorems of §2 and the self-duality theorem of §4, the senior author simply transcribed the first and quoted the second to give the main points of the calculation. That obscures the conceptual simplicity of the idea and its implementation. We explain in this section how the general theory applies. A punch line, explained at the end of the section, is that the conceptual argument applies to much more sophisticated cobordism theories, where the actual calculations are far more difficult. We take all homology and cohomology with coefficients in $\mathbb{F}_2$ in this section.

Recall the description of the Hopf algebra $H^*(BO)$ from (4.2). The structure of the dual Hopf algebra $H_*(BO)$ is given in Theorem 4.5. To conform to the notation of [**?**, Ch. 25], write $\gamma_i = b_i$. It is the image in $H_*(BO)$ of the nonzero class $x_i \in H_*(\mathbb{R}P^\infty)$. Thus $H_*(BO)$ is the polynomial algebra on the b_i, and $\psi(b_k) = \sum_{i+j=k} b_i \otimes b_j$.

The Thom prespectrum TO and its associated Thom spectrum MO are described in [**?**, pp. 216, 229], but we are not much concerned with the foundations of stable homotopy theory here. The ring structure on TO gives its homology an algebra structure, and the Thom isomorphism $\Phi\colon H_*(TO) \longrightarrow H_*(BO)$ is an isomorphism of algebras [**?**, p. 221]. Write $a_i = \Phi^{-1}(b_i)$. The Thom space $TO(1)$ of the universal line bundle is equivalent to $\mathbb{R}P^\infty$ and, with $a_0 = 1$, a_i is the image of x_{i+1} in $H_*(TO)$.

Let A be the mod 2 Steenrod algebra and A_* be its dual. Then A acts on the cohomology of spaces, prespectra, and spectra, and the action of A on the cohomology of a ring prespectrum T dualizes to give $H_*(T)$ a structure of left A-comodule algebra, as in Theorem 2.2. The composite

$$\pi = (\mathrm{id} \otimes \varepsilon)\nu\colon H_*(TO) \longrightarrow A_* \otimes H_*(TO) \longrightarrow A_*$$

is computed on [**?**, p. 224]. The computation just translates the easy computation of the action of A on $H^*(\mathbb{R}P^\infty)$ to a formula for the coaction of A_*. As an algebra, A_* is a polynomial algebra on certain generators ξ_r of degree $2^r - 1$, and $\pi(a_{2^r-1}) = \xi_r$. Thus π is an epimorphism.

By Theorem 2.2, this implies that there is an isomorphism

$$A_* \otimes P_{A_*}(H_*(TO)) \cong H_*(TO)$$

of left A_*-comodules and right $P_{A_*}(H_*(TO))$-modules. Since we know that A_* and $H_*(TO)$ are polynomial algebras such that the generators of A_* map to some of the generators of $H_*(TO)$, it is clear that $P_{A_*}(H_*(TO)) \equiv N_*$ must be a polynomial algebra on (abstract) generators u_i of degree i, where $i > 1$ and $i \neq 2^r - 1$. Dually $H^*(TO) = H^*(MO)$ is isomorphic as an A-module to $A \otimes N^*$. As explained informally in [**?**, §25.7], this implies that MO is a product of suspensions of Eilenberg-Mac Lane spectrum $H\mathbb{F}_2$ and that $\pi_*(MO) \cong N_*$ as an algebra. This gives the now standard way of obtaining Thom's calculation [**?**] of $\pi_*(MO)$.

The theorem applies to unoriented smooth manifolds, but one might consider less structured manifolds, such as piecewise linear or topological manifolds. Focusing on PL manifolds for definiteness, which makes sense since the theory of PL-manifolds was designed to get around the lack of obvious transversality in the theory of topological manifolds, one can adapt Thom's theorem to prove geometrically that the PL-cobordism groups are isomorphic to the homotopy groups of a Thom prespectrum TPL. By neglect of structure, we obtain a map of Thom prespectra $TO \longrightarrow TPL$. We have the same formal structure on TPL as we have on TO, and we have a commutative diagram

$$\begin{tikzcd}
H_*(TO) \arrow[rr] \arrow[dr, "\pi"'] & & H_*(TPL) \arrow[dl, "\pi"] \\
& A_* &
\end{tikzcd}$$

Even without any calculational knowledge of $H_*(BPL)$ and $H_*(TPL)$, we conclude that π on the right must also be an epimorphism.

Therefore, as a matter of algebra, Theorem 2.2 gives us an isomorphism

$$A_* \otimes P_{A_*}(H_*(TPL)) \cong H_*(TPL)$$

of left A_*-comodules and right $P_{A_*}H_*(TPL)$-algebras. Here again, the Thom isomorphism $\Phi\colon H_*(TPL) \longrightarrow H_*(BPL)$ is an isomorphism of algebras. Therefore, if we can compute $H_*(BPL)$ as an algebra, then we can read off what $P_{A_*}(H_*(TPL))$ must be as an algebra. The same formal argument as for MO shows that MPL is a product of suspensions of $H\mathbb{F}_2$ and that $\pi_*(MPL) \cong P_{A_*}(H_*(TPL))$ as algebras. In fact, this argument was understood and explained in [**?**] well before $H_*(BPL)$ was determined. The calculation of $H_*(BPL;\mathbb{F}_p)$ at all primes p is described in [**?**, **?**], but that is another story.[2] In any case, this sketch should give some idea of the algebraic power of the splitting theorems in §2.

6. A proof of the Bott periodicity theorem

The self duality of $H^*(BU)$ described in (4.1) and Theorem 4.3 also plays a central role in a quick proof of (complex) Bott periodicity. We describe how that works in this section. As discussed briefly in [**?**, §24.2], the essential point is to prove the following result. Homology and cohomology are to be taken with coefficients in $\mathbb{Z}$ in this section.

THEOREM 6.1. *There is a map $\beta\colon BU \longrightarrow \Omega SU$ of H-spaces which induces an isomorphism on homology.*

It follows from the dual Whitehead theorem that β must be an equivalence.

We begin by defining the Bott map β, following Bott [**?**]. Write $U(V)$ for the compact Lie group of unitary transformations $V \longrightarrow V$ on a complex vector space V with a given Hermitian product. If V is of countable dimension, let $U(V)$ denote the colimit of the $U(W)$ where W runs through the finite dimensional subspaces of V with their induced Hermitian products. Fixing the standard inclusions $\mathbb{C}^n \longrightarrow \mathbb{C}^\infty$, we specify $BU = U/U \times U$ to be the colimit of the Grassmannians $U(2n)/U(n) \times U(n)$. We let U be the colimit of the $U(2n)$ and SU be its subgroup colim $SU(2n)$ of unitary transformations with determinant one. For convenience, we write $\mathbb{V} = \mathbb{C}^\infty$ and let $\mathbb{V}^n$ denote the direct sum of n copies of $\mathbb{V}$.

It is also convenient to use paths and loops of length π. Taking $0 \le \theta \le \pi$, define $\nu(\theta) \in U(\mathbb{V}^2)$ by

$$\nu(\theta)(z', z'') = (e^{i\theta}z', e^{-i\theta}z'').$$

Note that $\nu(0)$ is multiplication by 1, $\nu(\pi)$ is multiplication by -1, and $\nu(\theta)^{-1} = \nu(-\theta)$. Define

$$\beta\colon U(\mathbb{C}^\infty \oplus \mathbb{C}^\infty) \longrightarrow \Omega SU(\mathbb{C}^\infty \oplus \mathbb{C}^\infty)$$

by letting

$$\beta(T)(\theta) = [T, \nu(\theta)] = T\nu(\theta)T^{-1}\nu(-\theta)$$

where $T \in U(\mathbb{V}^2)$. Clearly $[T, \nu(\theta)]$ has determinant one and $\beta(T)$ is a loop at the identity element e of the group $SU(\mathbb{V}^2)$. Moreover, since $\nu(\theta)$ is just a scalar multiplication on each summand $\mathbb{V}$, if $T = T' \times T'' \in U(\mathbb{V}) \times U(\mathbb{V})$, then $\beta(T)(\theta) = e$. Therefore β passes to orbits to give a well-defined map

$$\beta\colon BU = U/U \times U \longrightarrow \Omega SU.$$

[2] It is part of the 1970's story of infinite loop space theory and E_∞ ring spectra; see [**?**] for a 1970's overview and [**?**] for a modernized perspective.

To define the H-space structure on BU, choose a linear isometric isomorphism $\xi\colon \mathbb{V}^2 \longrightarrow \mathbb{V}$ and let the product T_1T_2 be the composite

$$\mathbb{V}^2 \xrightarrow{(\xi^{-1})^2} \mathbb{V}^4 \xrightarrow{T_1\oplus T_2} \mathbb{V}^4 \xrightarrow{\mathrm{id}\,\oplus\gamma\oplus\mathrm{id}} \mathbb{V}^4 \xrightarrow{\xi^2} \mathbb{V}^2,$$

where $\gamma\colon \mathbb{V}^2 \longrightarrow \mathbb{V}^2$ interchanges the two summands. Up to homotopy, the product is independent of the choice of ξ. The H-space structure we use on ΩSU is the pointwise product, $(\omega_1\omega_2)(\theta) = \omega_1(\theta)\omega_2\theta$. We leave it as an exercise to verify that β is an H-map.[3]

Let $\{e_i'\}$ and $\{e_i''\}$ denote the standard bases of two copies of $\mathbb{V}$ and let $\mathbb{C}_1^n$ and $\mathbb{C}_2^n$ be spanned by the first n vectors in each of these bases. Let

$$j\colon U(\mathbb{C}_1^n \oplus \mathbb{C}_2^1) \longrightarrow U(\mathbb{C}_1^n \oplus \mathbb{C}_2^n)$$

be the inclusion. Restrictions of β give a commutative diagram

$$\begin{tikzcd}
\mathbb{C}P^n = U(\mathbb{C}_1^n \oplus \mathbb{C}_2^1)/U(\mathbb{C}_1^n)\times U(\mathbb{C}_2^1) \arrow[r, "\alpha"] \arrow[d, "j"'] & \Omega SU(\mathbb{C}_1^n \oplus \mathbb{C}_2^1) = \Omega SU(n+1) \arrow[d, "\Omega j"] \\
U(2n)/U(n)\times U(n) = U(\mathbb{C}_1^n \oplus \mathbb{C}_2^n)/U(\mathbb{C}_1^n)\times U(\mathbb{C}_2^n) \arrow[r, "\beta"] & \Omega SU(\mathbb{C}_1^n \oplus \mathbb{C}_2^n) = \Omega SU(2n).
\end{tikzcd}$$

Passing to colimits over n, we obtain the commutative diagram

$$\begin{tikzcd}
\mathbb{C}P^\infty \arrow[r, "\alpha"] \arrow[d, "j"'] & \Omega SU \arrow[d, "\Omega j", "\simeq"'] \\
BU \arrow[r, "\beta"] & \Omega SU.
\end{tikzcd}$$

The right arrow is an equivalence, as we see from a quick check of homology or homotopy groups.

We claim that $H_*(\Omega SU)$ is a polynomial algebra on generators δ_i of degree $2i$, $i \geq 1$, and that $\alpha_*\colon H_*(\mathbb{C}P^\infty) \longrightarrow H_*(\Omega SU)$ is a monomorphism onto the free abelian group spanned by suitably chosen polynomial generators δ_i. The algebra in §4 implies the topological statement that $j_*\colon H_*(\mathbb{C}P^\infty) \longrightarrow H_*(BU)$ is a monomorphism onto the free abelian group generated by a set $\{\gamma_i\}$ of polynomial generators for $H_*(BU)$, hence the claim will complete the proof of Theorem 6.1.

Think of S^1 as the quotient of $[0,\pi]$ obtained by setting $0 = \pi$. Let

$$i\colon U(\mathbb{C}_1^{n-1} \oplus \mathbb{C}_2^1) \longrightarrow U(\mathbb{C}_1^n \oplus \mathbb{C}_2^1)$$

be the inclusion. It induces a map $i\colon \mathbb{C}P^{n-1} \longrightarrow \mathbb{C}P^n$ that leads to the left diagram below, and the right diagram is its adjoint.

(6.2)
$$\begin{tikzcd}
\mathbb{C}P^{n-1} \arrow[r, "\alpha"] \arrow[d, "i"'] & \Omega SU(n) \arrow[d, "\Omega i"] & \Sigma\mathbb{C}P^{n-1} \arrow[r, "\hat{\alpha}"] \arrow[d, "\Sigma i"'] & SU(n) \arrow[d, "i"] \\
\mathbb{C}P^n \arrow[r, "\alpha"] \arrow[d, "\rho"'] & \Omega SU(n+1) \arrow[d, "\Omega\pi"] & \Sigma\mathbb{C}P^n \arrow[r, "\hat{\alpha}"] \arrow[d, "\Sigma\rho"'] & SU(n+1) \arrow[d, "\pi"] \\
S^{2n} \arrow[r, "h"'] & \Omega S^{2n+1} & \Sigma S^{2n} \arrow[r, "\hat{h}"'] & S^{2n+1}
\end{tikzcd}$$

[3] This is also part of the 1970's infinite loop space story; details generalizing these H-space structures and maps to the context of actions by an E_∞ operad may be found in [**?**, pp. 9-17].

Here $\rho\colon \mathbb{C}P^n \longrightarrow \mathbb{C}P^n/\mathbb{C}P^{n-1} \cong S^{2n}$ is the quotient map and $\pi(T) = T(e'_n)$.

LEMMA 6.3. *The composite $\Omega\pi \circ \alpha \circ i$ is trivial, so that $\Omega\pi \circ \alpha$ factors as the composite $h\rho$ for a map h. Moreover, the adjoint $\hat{h}$ of h is a homeomorphism.*

PROOF. Let $T \in U(\mathbb{C}^n_1 \oplus \mathbb{C}^1_2)$ represent $\bar{T} \in \mathbb{C}P^n$ and let T_1^{-1} and T_2^{-1} denote the projections of T^{-1} on $\mathbb{C}^n_1$ and on $\mathbb{C}^1_2$. We have

$$\begin{array}{rcl} (\Omega\pi)\alpha(T)(\theta) & = & T\nu(\theta)T^{-1}\nu(-\theta)(e'_n) \\ & = & T\nu(\theta)T^{-1}(e^{-i\theta}e'_n) \\ & = & T(T_1^{-1}(e'_n), e^{-2i\theta}T_2^{-1}(e'_n)) \\ & = & e'_n + (e^{-2i\theta} - 1)TT_2^{-1}(e'_n) \end{array}$$

as we see by adding and subtracting $TT_2^{-1}(e'_n)$. If $T(e'_n) = e'_n$, so that T is in the image of $U(\mathbb{C}^{n-1}_1 \oplus \mathbb{C}^1_2)$ and $\bar{T}$ is in the image of $\mathbb{C}P^{n-1}$, then $T_2^{-1}(e'_n) = 0$ and thus $(\Omega\pi)\alpha(T)(\theta) = e'_n$ for all θ. To prove that $\hat{h}$ is a homeomorphism, it suffices to check that it is injective. Its image will then be open by invariance of domain and closed by the compactness of ΣS^{2n}, hence will be all of S^{2n+1} since S^{2n+1} is connected. Denote points of ΣX as $[x, \theta]$ for $x \in X$ and $\theta \in S^1$. We have

$$\hat{h}(\Sigma\rho)[\bar{T}, \theta] = \pi\hat{\alpha}[\bar{T}, \theta] = (\Omega\pi)\alpha(T)(\theta) = e'_n + (e^{-2i\theta} - 1)TT_2^{-1}(e'_n).$$

Since T^{-1} is the conjugate transpose of T, $T_2^{-1}(e'_n) = \bar{c}e''_1$, where c is the coefficient of e'_n in $T(e''_1)$. Here $T \notin \mathbb{C}P^{n-1}$ if and only if $c \neq 0$. and then $TT_2^{-1}(e'_n) = e'_n + T'(e'_n)$, where T' denotes the projection of T on $\mathbb{C}^{n-1} \oplus \mathbb{C}^1_2$. Therefore

$$\hat{h}[\rho(\bar{T}), \theta] = e^{-2i\theta}e'_n + T'(e'_n)$$

when $\bar{T} \notin \mathbb{C}P^{n-1}$. The injectivity is clear from this. □

Armed with this elementary geometry, we return to homology. The rightmost column in the second diagram of (6.2) is a fibration, and we use it to compute $H_*(\Omega SU(n+1))$ by induction on n. We have $SU(2) \cong S^3$, and we claim inductively that the cohomology Serre spectral sequence of this fibration satisfies $E_2 = E_\infty$. This leads to a quick proof that

$$H_*(SU(n+1)) = E\{y_{2i+1} | 1 \leq i \leq n\}$$

as a Hopf algebra, where y_{2i+1} has degree $2i + 1$ and $\pi_*(y_{2n+1})$ is a generator of $H_{2n+1}(S^{2n+1})$. Indeed, assume that we know this for $SU(n)$. Then, since the cohomology spectral sequence is multiplicative and the exterior algebra generators of $H^*(SU(n)) = E_2^{0,*}$ have degrees less than $2n$, they must be permanent cycles. Therefore $E_2 = E_\infty$. This implies that $H^*(SU(n+1))$ is an exterior algebra. Moreover, by the edge homomorphisms, i^* is an isomorphism in degrees less than $2n+1$ and the last exterior algebra generator is $\pi^*(i_{2n+1})$. Inductively, the exterior generators in degrees less than $2n$ are primitive. Since i is a map of topological groups, $i*$ is a map of Hopf algebras. Since $i^*\pi^* = 0$, inspection of the coproduct shows that the generator in degree $2n + 1$ must also be primitive.

Using the Serre spectral sequence of the path space fibration over $SU(n + 1)$, we conclude that

$$H_*(\Omega SU(n+1)) \cong P\{\delta_i | 1 \leq i \leq n\},$$

where δ_i has degree $2i$. The classical way to see this is to construct a test multiplicative spectral sequence with

$$E^2_{*,*} = P\{\delta_i | 1 \le i \le n\} \otimes E\{y_{2i+1} | 1 \le i \le n\}$$

and with differentials specified by requiring y_{2i+1} to transgress to δ_i. This ensures that E_∞ is zero except for $\mathbb{Z} = E^\infty_{0,0}$. We can map the test spectral sequence to the homology Serre spectral sequence of the path space fibration by a map that is the identity on $E^2_{0,*}$ and commutes with the transgression. The conclusion follows by the comparison theorem, **??**. The argument shows that the polynomial generators transgress to the exterior algebra generators and thus that the exterior algebra generators suspend to the polynomial algebra generators. At the risk of belaboring the obvious, we spell things out explicitly via the following commutative diagram, in which the unlabelled isomorphisms are suspension isomorphisms.

$$\begin{tikzcd}
H_{2n}(\mathbb{C}P^n) \arrow[rrr, "\alpha_*"] \arrow[ddddd, "\rho_*"', "\cong"] \arrow[ddr, "\cong"'] & & & H_{2n}(\Omega SU(n+1)) \arrow[dl, "\cong"'] \arrow[ddl, "\sigma"] \arrow[ddddd, "(\Omega\pi)_*"] \\
& & H_{2n+1}(\Sigma\Omega SU(n+1)) \arrow[d, "\varepsilon_*"] & \\
& H_{2n+1}(\Sigma\mathbb{C}P^n) \arrow[ur, "(\Sigma\alpha)_*"] \arrow[r, "\hat{\alpha}_*"'] \arrow[d, "(\Sigma\rho)_*"', "\cong"] & H_{2n+1}(SU(n+1)) \arrow[d, "\pi_*"] & \\
& H_{2n+1}(\Sigma S^{2n}) \arrow[r, "\hat{h}_*", "\cong"'] \arrow[dr, "(\Sigma h)_*"'] & H_{2n+1}(S^{2n+1}) & \\
& & H_{2n+1}(\Sigma\Omega S^{2n+1}) \arrow[u, "\varepsilon_*"'] & \\
H_{2n}(S^{2n}) \arrow[rrr, "h_*"'] \arrow[uur, "\cong"] & & & H_{2n}(\Omega S^{2n+1}) \arrow[ull, "\sigma"'] \arrow[ul, "\cong"]
\end{tikzcd}$$

Here ε denotes the evaluation map of the (Σ, Ω) adjunction, and the suspension σ is defined to be the composite of ε_* and the suspension isomorphism. The algebra generator δ_n maps to a fundamental class under $\pi_*\sigma$. By the diagram, so does the basis element $x_{2n} \in H_{2n}(\mathbb{C}P^n)$. Therefore, modulo decomposable elements which are annihilated by σ, $\alpha_*(x_{2i}) = \delta_i$ as claimed.

CHAPTER 3

Lie algebras and Hopf algebras in characteristic zero

All of the structure theorems for Hopf algebras in common use in algebraic topology are best derived by filtration techniques from the Poincaré-Birkhoff-Witt theorem for graded Lie algebras and restricted Lie algebras. In this chapter, we first introduce Lie algebras and prove the PBW theorem for their universal enveloping algebras. We next show that primitive (= primitively generated) Hopf algebras in characteristic zero are the universal enveloping algebras of their Lie algebras of primitive elements. We then use this fact to study the algebra structure of commutative Hopf algebras in characteristic zero.

While some of these results first appeared in Milnor and Moore [**?**], the most basic structure theorems go back to earlier work of Hopf, Leray, and Borel.

1. Graded Lie algebras

We continue to work over a fixed commutative ring R. The following witty definition is due to John Moore and used in [**?**].

Definition 1.1. A (graded) Lie algebra over R is a (graded) R-module L together with a morphism of R-modules $L \otimes L \to L$, denoted $[-,-]$ and called the bracket operation, such that there exists an associative R-algebra A and a monomorphism of R-modules $j : L \to A$ such that $j([x,y]) = [jx, jy]$ for $x, y \in L$, where the bracket operation in A is the (graded) commutator,

$$[a,b] = ab - (-1)^{\deg a \deg b} ba.$$

A morphism of Lie algebras is a morphism of R-modules which commutes with the bracket operation.

The following identities are immediate consequences of the definition. It would be more usual to take them as the defining properties of the bracket operation, but we shall see that for particular ground rings R the definition can imply more relations than are listed.

Lemma 1.2. *Let L be a Lie algebra and let $x \in L_p$, $y \in L_q$, and $z \in L_r$. Then the following identities hold.*

(i) $[x,y] = -(-1)^{pq}[y,x]$

(ii) $[x,x] = 0$ *if either* $\operatorname{char} R = 2$ *or p is even*

(iii) $(-1)^{pr}[x,[y,z]] + (-1)^{pq}[y,[z,x]] + (-1)^{rq}[z,[x,y]] = 0$

(iv) $[x,[x,x]] = 0$ *if p is odd.*

Formula (iii) is called the Jacobi identity. When p is even, (i) implies $2[x,x] = 0$; when p is odd, (iii) implies $3[x,[x,x]] = 0$. We shall see that, at least if R is a field, any R-module with a bracket operation satisfying these identities can be embedded in a bracket-preserving way in an associative algebra and is therefore a Lie algebra. This is not true for a general R. For instance, $[x, 2x] = 0$ if $\operatorname{char} R = 4$ is an identity not implied by those of the lemma (when $\deg(x)$ is odd). Of course, for any R, any associative alegbra is a Lie algebra under the commutator operation.

Definition 1.3. The universal enveloping algebra of a Lie algebra L is an associative algebra $U(L)$ together with a morphism of Lie algebras $i : L \to U(L)$ such that, for any morphism of Lie algebras $f : L \to A$, where A is an associative algebra, there exists a unique morphism of algebras $\tilde{f} : U(L) \to A$ such that $\tilde{f}i = f$.

Clearly $U(L)$ is unique up to canonical isomorphism, if it exists.

Proposition 1.4. *Any Lie algebra L has a universal enveloping algebra $U(L)$, and $i : L \to U(L)$ is a monomorphism whose image generates $U(L)$ as an algebra. Moreover, $U(L)$ is a primitive Hopf algebra.*

Proof. Let $T(L)$ be the tensor algebra, or free associative algebra, generated by L. Explicitly, $T(L) = \sum_{n\geq 0} T_n(L)$, where $T_0(L) = R$ and $T_n(L) = L \otimes \ldots \otimes L$, n factors L, if $n > 0$. The product in $T(L)$ is obtained by passage to direct sums from the evident isomorphisms $T_m(L) \otimes T_n(L) \to T_{m+n}(L)$. Define $i : L \to T(L)$ to be the identification of L with $T_1(L)$. For an associative algebra A, a map of R-modules $f : L \to A$ extends uniquely to a map of algebras $\tilde{f} : T(L) \to A$. Let I be the two-sided ideal in $T(L)$ generated by the elements

$$xy - (-1)^{\deg x \deg y} yx - [x, y],\ \ x, y \in L,$$

define $U(L) = T(L)/I$, and let $i : L \to U(L)$ be the evident composite. Clearly i has the required universal property. Of course, the injectivity of i is built into our definition of a Lie algebra, and $i(L)$ generates $U(L)$ since $i(L)$ generates $T(L)$. By the universal property, a morphism $f : L \to L'$ of Lie algebras induces a unique morphism $U(f)$ of associative algebras such that the following diagram commutes.

$$\begin{tikzcd}
L \arrow[r, "f"] \arrow[d, "i"] & L' \arrow[d, "i'"] \\
U(L) \arrow[r, "U(f)"] & U(L')
\end{tikzcd}$$

If we take $L' = \{0\}$, then $U(L') = R$ and we obtain an an augmentation of $U(L)$. The product $L \times L'$ of Lie algebras inherits a structure of Lie algebra, and the algebra $U(L) \otimes U(L')$ together with the evident morphism $i : L \times L' \to U(L) \otimes U(L')$,

$$i(x, x') = x \otimes 1 + 1 \otimes x'$$

is easily checked to satisfy the universal property that defines $U(L \times L')$. The diagonal $\triangle : L \to L \times L$ is a map of Lie algebras and therefore induces a morphism of algebras $\psi : U(L) \to U(L) \otimes U(L)$ such that the following diagram commutes.

$$\begin{tikzcd}
L \arrow[r, "\triangle"] \arrow[d, "i"] & L \times L \arrow[d, "i"] \\
U(L) \arrow[r, "\psi"] & U(L) \otimes U(L)
\end{tikzcd}$$

Thus $U(L)$ is a bialgebra, and $i(L) \subset PU(L)$ by the diagram, so that $U(L)$ is primitive. For the antipode, we have the opposite Lie algebra L^{op} with bracket $[-,-]\gamma$, and $x \longrightarrow -x$ defines a map of Lie algebras $L \longrightarrow L^{\mathrm{op}}$. We can identify $U(L^{\mathrm{op}})$ as $U(L)^{op}$, and then the universal property gives a map of algebras $\chi\colon U(L) \longrightarrow U(L)^{op}$, that is, an involution on $U(L)$ itself. Writing the obvious equalities $[x,-x] = 0 = [-x,x]$ as diagrams and passing to the corresponding diagrams induced on the level of universal enveloping algebras, we see that χ is an antipode on $U(L)$. □

2. The Poincaré-Birkhoff-Witt theorem

The Poincaré-Birkhoff-Witt theorem gives a complete description of the associated graded Hopf algebra of $U(L)$ with respect to a suitable filtration (under appropriate hypotheses) and therefore gives a complete description of the additive structure of $U(L)$. We require a definition.

Definition 2.1. Let L be a Lie algebra. The Lie filtration of $U(L)$ is specified by $F_pU(L) = 0$ if $p < 0$, $F_0U(L) = R$, and $F_pU(L) = (R \oplus L)^p$ if $p \geq 1$. Clearly $U(L) = \cup_p F_pU(L)$, so the filtration is complete.

Provided that the Lie filtration is split or flat, so that $E^0(U(L) \otimes U(L))$ is isomorphic to $E^0U(L) \otimes E^0U(L)$, $E^0U(L)$ inherits a structure of primitive Hopf algebra from $U(L)$. Since the commutator in $U(L)$ of elements in L agrees with the bracket operation in L and since L generates $U(L)$, we see immediately that $E^0U(L)$ is commutative. Clearly we have

$$QE^0U(L) = E^0_{1,*}U(L) = L, \quad \text{where} \quad E^0_{1,q}U(L) = L_{q+1}.$$

Let $L^\sharp$ denote the underlying R-module of L regarded as an abelian Lie algebra and write $A(L) = U(L^\sharp)$. Then $A(L)$ is the free commutative algebra generated by L. Explicitly, $A(L) = T(L)/J$ where J is the commutator ideal.

For a filtered R-module A, write $E^\oplus A$ for the graded R-module that is obtained by regrading the associated bigraded R-module E^0A by total degree:

$$E^\oplus_n A = \sum_{p+q=n} E^0_{p,q}A.$$

If E^0A is a bigraded algebra, Hopf algebra, etc, then $E^\oplus A$ is a graded algebra, Hopf algebra, etc.

By the universal property of $A(L)$, the evident inclusion of L in $E^\oplus U(L)$ induces a natural map of commutative algebras $f : A(L) \to E^\oplus U(L)$.

Notation 2.2. If $\operatorname{char} R = 2$, let $L^+ = L$ and $L^- = \{0\}$. If $\operatorname{char} R \neq 2$, let L^+ and L^- be the R-submodules of L concentrated in even and in odd degrees.

The hypotheses on the characteristic of R in the next result ensure that the identities of Lemma 1.2 suffice to characterize our Lie algebras, as we shall see.

Theorem 2.3 (Poincaré-Birkhoff-Witt). *Let L be an R-free Lie algebra. Assume that $\operatorname{char} R = 2$, or that 2 is invertible in R, or that $L = L^+$ so that L is concentrated in even degrees. Then $f : A(L) \to E^\oplus U(L)$ is an isomorphism of Hopf algebras.*

PROOF. It will fall out of the proof that the Lie filtration of $U(L)$ is split, so that $E^{\oplus}U(L)$ is a primitively generated Hopf algebra, and f will preserve coproducts since it is the identity on the R-module L of primitive generators. Of course, f is an epimorphism since L generates $E^{\oplus}U(L)$. Filter $E^{\oplus}U(L)$ by filtration degree,

$$F_pE^{\oplus}U(L) = \sum_{i\leq p} E^0_{i,*}U(L).$$

Obviously $E^0E^{\oplus}U(L) = E^0U(L)$. Give $A(L)$ its Lie filtration. Clearly $E^0A(L)$ is the free commutative bigraded algebra generated by L regarded as a bigraded R-module via $L_{1,q} = L_{q+1}$. The map f is filtration-preserving, and it suffices to prove that E^0f is a monomorphism.

Give $T(L)$ the evident filtration, $F_pT(L) = \sum_{n\leq p} T_n(L)$, and observe that the quotient maps $\pi : T(L) \to A(L)$ and $\rho : T(L) \to U(L)$ are both filtration-preserving. Let $I = \ker\rho$. We shall construct a filtration preserving morphism of R-modules $\sigma : T(L) \to A(L)$ such that $\sigma(I) = 0$ and $E^0\sigma = E^0\pi$. It will follow that σ factors as $\bar{\sigma}\rho$ for a filtration preserving R-map $\bar{\sigma} : U(L) \to A(L)$. We will have $E^0\bar{\sigma}E^0\rho = E^0\pi$ and, since $E^0\rho$ and $E^0\pi$ are epimorphisms of algebras, $E^0\bar{\sigma}$ will be a morphism of algebras. The composite

$$E^0A(L) \xrightarrow{E^0f} E^0U(L) \xrightarrow{E^0\bar{\sigma}} E^0A(L)$$

will be the identity since it will be a morphism of algebras which restricts to the identity on the R-module L of generators. Thus E^0f will be a monomorphism and the proof will be complete.

To construct σ, let $\{z_k\}$ be an R-basis for L indexed on a totally ordered set. The set of monomials

$$\{z_{k_1}\dots z_{k_n} | k_1 \leq \dots \leq k_n \text{ and } k_i < k_{i+1} \text{ if } z_{k_i} \in L^-\} \tag{2.4}$$

is an R-basis for $A(L)$. Let y_k denote z_k regarded as an element of $T(L)$. Then $y_{k_1}\dots y_{k_n}$ is a typical basis element of $T_n(L)$. Of course, the sequence $\{k_1, \dots, k_n\}$ will generally not be ordered as in (2.4). When it is so ordered, we require σ to satisfy the formula

$$\sigma(y_{k_1}\dots y_{k_n}) = z_{k_1}\dots z_{k_n} \text{ if } k_1 \leq \dots \leq k_n \text{ and } k_i < k_{i+1} \text{ if } z_{k_i} \in L^-; \tag{2.5}$$

For a general sequence $\{k_1, \dots, k_n\}$ and $1 \leq i < n$, we require

$$\begin{aligned} \sigma(y_{k_1}\dots y_{k_n}) &= (-1)^{\deg z_{k_i} \deg z_{k_{i+1}}}\sigma(y_{k_i}\dots y_{k_{i-1}}y_{k_{i+1}}y_{k_i}y_{k_{i+2}}\dots y_{k_n}) \\ &\quad + \sigma(y_{k_1}\dots y_{k_{i-1}}[y_{k_i}, y_{k_{i+1}}]y_{k_{i+2}}\dots y_{k_n}). \end{aligned} \tag{2.6}$$

Clearly, if there is a well-defined map $\sigma\colon T(L) \longrightarrow A(L)$ of R-modules that satisfies these formulae, the desired relations $I \subset \ker\sigma$ and $E^0\sigma = E^0\pi$ will follow.

We define $\sigma : T(L) \to A(L)$ by induction on the filtration degree n, with $\sigma(1) = 1$ and $\sigma(y_k) = z_k$ handling filtration degrees 0 and 1. Assume that σ has been defined on $F_{n-1}T(L)$. Define the index q of a sequence $\{k_1, \dots, k_n\}$ to be the number of transpositions required to put it in non-decreasing order. We define σ by induction on n and, for fixed n, by induction on the index q. We have defined σ for $n \leq 1$, so we assume that $n > 1$. Define σ by (2.5) for sequences of index 0 unless some $k_i = k_{i+1}$ with $z_{k_i} \in L^-$, in which case define σ by the formula

$$\sigma(y_{k_1}\dots y_{k_n}) = \frac{1}{2}\sigma(y_{k_1}\dots y_{k_{i-1}}[y_{k_i}, y_{k_i}]y_{k_{i+2}}\dots y_{k_n}). \tag{2.7}$$

Observe that (2.7) is consistent with and in fact forced by (2.6). Assuming that σ has been defined on sequences of index less than q and that $\{k_1, \ldots, k_n\}$ has index q, we define $\sigma(y_{k_1} \ldots y_{k_n})$ by (2.6) if $k_i > k_{i+1}$ and by (2.7) if $k_i = k_{i+1}$ and $z_{k_i} \in L^-$. To complete the proof, we must show that σ is actually well-defined, that is, that our definition of σ by (2.6) and (2.7) is independent of the choice of i. The argument is tedious, but elementary, and we shall not give full details. There are four cases to be checked, each with two subcases.

Case 1. $k_i = k_{i+1}$ and $k_j = k_{j+1}$, $j \geq i+1$, with $z_{k_i} \in L^-$ and $z_{k_j} \in L^-$.

Subcase $j > i+1$. We must show that

$$\sigma(y_{k_1} \ldots [y_{k_i}, y_{k_i}] \ldots y_{k_n}) = \sigma(y_{k_1} \ldots [y_{k_j}, y_{k_j}] \ldots y_{k_n}).$$

Here (2.6) and induction on n show that both sides are equal to

$$\frac{1}{2}\sigma(y_1 \ldots [y_{k_i}, y_{k_i}] \ldots [y_{k_j}, y_{k_j}] \ldots y_{k_n}).$$

Subcase $j = i+1$. Here (2.6), induction on n, and the identity $[x,[x,x]] = 0$ imply the equality

$$\sigma(y_{k_1} \ldots y_{k_i}[y_{k_i}, y_{k_i}] \ldots y_{k_n}) = \sigma(y_{k_1} \ldots [y_{k_i}, y_{k_i}]y_{k_i} \ldots y_{k_n}).$$

Case 2. $k_i = k_{i+1}$ with $z_{k_i} \in L^-$ and $k_j > k_{j+1}$, $j \geq i+1$.

Subcase $j > i+1$**.** The argument here is similar to (but has more terms to check than) the argument in the subcase $j > i+1$ of Case 1, the induction hypotheses on both n and q being required.

Subcase $j = i+1$**.** Let $u = y_{k_i} = y_{k+1}$ and $v = y_{k_{i+2}}$ and let $\deg v = p$; of course, $\deg u$ is odd. We must show that

$$\frac{1}{2}\sigma(y_{k_1} \ldots [u,u]v \ldots y_{k_n}) = (-1)^p\sigma(y_{k_1} \ldots uvu \ldots y_{k_n}) + \sigma(y_{k_1} \ldots u[u,v] \ldots y_{k_n}).$$

By (2.6) and induction on q and n, we have

$$\begin{array}{rcl} \sigma(y_{k_1} \ldots uvu \ldots y_{k_n}) & = & (-1)^p\sigma(y_{k_1} \ldots vuu \ldots y_{k_n}) + \sigma(y_{k_1} \ldots [u,v]u \ldots y_{k_n}) \\ & = & \frac{1}{2}(-1)^p\sigma(y_{k_1} \ldots v[u,u] \ldots y_{k_n}) + \sigma(y_{k_1} \ldots [u,v]u \ldots y_{k_n}) \\ & = & \frac{1}{2}(-1)^p(\sigma(y_{k_1} \ldots [u,u]v \ldots y_{k_n}) + \sigma(y_{k_1} \ldots [v,[u,u]] \ldots y_{k_n})) \\ & & -(-1)^p\sigma(y_{k_1} \ldots u[u,v] \ldots y_{k_n}) + \sigma(y_{k_1} \ldots [[u,v],u] \ldots y_{k_n}). \end{array}$$

The Jacobi and anticommutativity formulas imply

$$\begin{array}{rcl} \frac{1}{2}[v,[u,u]] + (-1)^p[[u,v],u] & = & \frac{1}{2}[v,[u,u]] + [u,[u,v]] \\ & = & \frac{1}{2}([v,[u,u]] - (-1)^p[u,[v,u]] + [u,[u,v]]) = 0. \end{array}$$

Comparing formulas, we obtain the desired equality.

Case 3. $k_i > k_{i+1}$ and $k_j = k_{j+1}$ with $z_k \in L^-$, $j \geq i+1$.

The proof in this case is symmetric to that in case 2.

Case 4. $k_i > k_{i+1}$ and $k_j > k_{j+1}$ with $j \geq i+1$.

The proof when $j > i+1$ is straightforward by induction, as in the subcase $j > i+1$ of Case 1, and the proof when $j = i+1$ is a calculation similar to that in the subcase $j = i+1$ of Case 2. □

We retain the hypotheses of the theorem in the following corollary.

COROLLARY 2.8. *Let $\{x_i\}$ and $\{y_j\}$ be R-bases for L^- and L^+ indexed on totally ordered sets. Then $U(L)$ is the free R-module on the basis*

$$\{x_{i_1}\dots x_{i_m} y_{j_1}^{r_1}\dots y_{j_n}^{r_n} | i_1 < \dots < i_m,\ j_1 < \dots < j_n \text{ and } r_k \geq 1\}.$$

PROOF. Since $E^{\oplus}U(L)$ is a free R-module, it is isomorphic as an R-module to $U(L)$. The conclusion follows from the evident analog for $U(L^\sharp) = A(L)$. □

COROLLARY 2.9. *Let L be a free R-module together with a bracket operation satisfying the identities listed in Lemma 1.2. Assume that* $\operatorname{char} R = 2$*, or 2 is invertible in R, or $L = L^+$. Then L is a Lie algebra.*

PROOF. Construct $U(L)$ as in the proof of Proposition 1.4 and give it the Lie filtration of Definition 2.1. The proof of Theorem 2.3 only used the cited identities and so gives that $A(L) \cong E^{\oplus}U(L)$. Thus $L \to U(L)$ is a bracket-preserving monomorphism of R-modules. □

3. Primitively generated Hopf algebras in characteristic zero

Throughout this section and the next, R is assumed to be a field of characteristic zero. However, all of the results remain valid if R is any ring of characteristic zero in which 2 is invertible and all R-modules in sight are R-free.

A quick calculation shows that the R-module PA of primitive elements of a Hopf algebra A is a sub Lie algebra. The universal property of $U(PA)$ thus gives a natural map of Hopf algebras $g : U(PA) \to A$, and g is clearly an epimorphism if A is primitive. Let $\mathscr{L}$ and $\mathscr{P}\mathscr{H}$ denote the categories of Lie algebras and of primitive Hopf algebras over R. We have functors $U : \mathscr{L} \to \mathscr{P}\mathscr{H}$ and $P : \mathscr{P}\mathscr{H} \to \mathscr{L}$, a natural inclusion $L \subset PU(L)$, and a natural epimorphism $g : U(PA) \to A$, where $L \in \mathscr{L}$ and $A \in \mathscr{P}\mathscr{H}$. This much would be true over any commutative ring R, but when R is a field of characteristic zero we have the following result.

THEOREM 3.1. *The functors $U : \mathscr{L} \to \mathscr{P}\mathscr{H}$ and $P : \mathscr{P}\mathscr{H} \to \mathscr{L}$ are inverse equivalences of categories. More explicitly,*

(i) $PU(L) = L$ for any Lie algebra L and
(ii) $g : U(PA) \to A$ is an isomorphism for any primitive Hopf algebra A.

PROOF. We first prove (i). Consider the Lie filtration of $U(L)$. Let $x \in F_pU(L)$, $x \notin F_{p-1}U(L)$, and suppose that $x \in PU(L)$. It suffices to prove that $p = 1$. The image of x in $E^0_{p.*}U(L)$ is primitive. By the PBW-theorem, $E^{\oplus}U(L) \cong A(L)$ as a Hopf algebra. Consider the basis for $A(L)$ given in Corollary 2.8. The generators x_i and y_j there are primitive. Using the notation (i, j) for the evident binomial coefficient considered as an element of R, we see that

$$\psi(y^n) = \sum_{i+j=n} (i,j) y^i \otimes y^j \quad \text{if} \quad y \in L^+.$$

Since $\operatorname{char} R = 0$, we check from this that no decomposable basis element is primitive and that no two basis elements have any summands of their coproducts in common, so that no linear combination of decomposable elements is primitive. This implies that $p = 1$ and proves (i).

To prove (ii), define the primitive filtration of a Hopf algebra A by

$$F_pA = 0 \text{ if } p < 0, \quad F_0A = A, \quad \text{and} \quad F_pA = (R \oplus PA)^p \text{ if } p > 0.$$

This filtration is complete, $A = \cup_p F_p A$, if and only if A is primitive. By (i), the Lie and primitive filtrations coincide on $U(L)$. For $A \in \mathscr{P}\mathscr{H}$ the epimorphism $g : U(PA) \to A$ is filtration-preserving and, since $PU(PA) = PA$, g is an isomorphism on the R-modules of primitive elements. Therefore $E^0 g$ is a monomorphism on the primitive elements of $E^0 U(PA)$, that is, on $E^0_{1,*}U(PA)$. Since $E^0 U(PA)$ is connected with respect to its filtration degree, $E^0 g$ is a monomorphism by Proposition 1.4 and g is a monomorphism by Proposition 1.1. □

We emphasize that A itself is not assumed to be connected here.

Corollary 3.2. *If A is a commutative primitive Hopf algebra, then A is isomorphic as a Hopf algebra to the free commutative algebra generated by PA.*

Proof. $A \cong U(PA) = A(PA)$ since PA is an abelian Lie algebra. □

Among other things, our next corollary shows that a connected Hopf algebra is primitive if and only if it is cocommutative.

Corollary 3.3. *Let A be a connected quasi Hopf algebra.*

(i) $\nu : PA \to QA$ is a monomorphism if and only if A is associative and commutative.

(ii) $\nu : PA \to QA$ is an epimorphism if and only if A is coassociative and cocommutative.

(iii) $\nu : PA \to QA$ is an isomorphism if and only if A is a commutative and cocommutative Hopf algebra.

Proof. By Lemma 1.1, if ν is a monomorphism then A is associative and commutative. Conversely, suppose that A is associative and commutative. Give A its product filtration (see Definition 2.9). Then $E^0 A$ is a commutative primitive Hopf algebra, hence $E^0 A \cong A(PE^0 A)$ by the previous corollary. It follows that $PE^0 A = E^0_{-1,*}A$. If $x \in PA$, $x \in F_p A$, and $x \notin F_{p-1}A$, then the image of x in $E^0_{p,*}A$ is primitive and we must have $p = -1$. This implies that ν is a monomorphism. When A is of finite type, (ii) follows from (i) by dualization since $A \cong A^{**}$ and (i) holds for A^*. The general case of (i) follows by passage to colimits, using Lemma 1.2, since the functors P and Q commute with (directed) colimits. Part (iii) follows from (i) and (ii). □

Corollary 3.4. *A sub Hopf algebra of a primitive Hopf algebra is primitive.*

Proof. Let $A \subset B$, where B is primitive. Since B is cocommutative, so is A. If A is connected, the conclusion follows from (ii) of the previous corollary. For the general case, let $A' = U(PA)$ and let $g : A' \to A$ be the natural map. Give A' and B their primitive filtrations and filter A by $F_p A = A \cap F_p B$. These filtrations are all complete, and g and the inclusion $A \to B$ are filtration-preserving. Clearly $F_1 A' = R \oplus PA = F_1 A$. The induced map $E^0 A \to E^0 B$ is again a monomorphism. Since $E^0 A$ is connected (with respect to its filtration degree) and cocommutative, it is primitively generated. Since $PE^0 B = E^0_{1,*}B$, we find

$$PE^0 A' = E^0_{1,*}A' \cong E^0_{1,*}A = PE^0 A.$$

Thus $E^0 g$ is an isomorphism on primitives and therefore also an epimorphism on indecomposables. By Propositions 1.3 and 1.4, this implies that $E^0 g$ is an isomorphism and thus g is an isomorphism. □

Corollary 3.5. *A sub Hopf algebra A of a primitive Hopf algebra B is a normal sub algebra if and only if PA is a Lie ideal of PB. When this holds, $B//A = U(PB/PA)$ and*

$$0 \longrightarrow PA \longrightarrow PB \longrightarrow P(B//A) \longrightarrow 0$$

is an exact sequence of Lie algebras.

Proof. Assume PA is a Lie ideal in PB. If $x \in PA$ and $y \in PB$, then $[x, y] \in PA$ and, since A is primitive, the equation $xy = [x, y] + (-l)^{\deg x \deg y} yx$ therefore implies that $IA \cdot B = B \cdot IA$. Conversely, assume that A is a normal sub algebra of B and let $C = B//A$. The exact sequence

$$0 \to PA \to PB \to PC$$

implies that PA is a Lie ideal of PB. It is easily checked that C and the inclusion $PB/PA \to C$ satisfy the universal property required of $U(PB/PA)$, and the remaining conclusions follow. □

4. Commutative Hopf algebras in characteristic zero

Again, let R be a field of characteristic zero. We prove the classical structure theorems for commutative Hopf algebras in characteristic zero. As before, $A(X)$ denotes the free commutative algebra generated by an R-module X. If we write $E(X)$ for the exterior algebra generated by an R-module X concentrated in odd degrees and $P(X)$ for the polynomial algebra generated by an R-module X concentrated in even degrees, then, for a general R-module X,

$$A(X) = E(X^-) \otimes P(X^+),$$

where X^- and X^+ denote the submodules of X concentrated in odd and even degrees, respectively.

Theorem 4.1 (Leray). *Let A be a connected, commutative, and associative quasi Hopf algebra. Let $\sigma : QA \to IA$ be a morphism of R-modules such that $\pi\sigma = \mathrm{id}$, where $\pi : IA \to QA$ is the quotient map. Then the morphism of algebras $f : A(QA) \to A$ induced by σ is an isomorphism.*

Proof. Give $A(QA)$ and A their product filtrations. These filtrations are complete since A is connected, and f is filtration-preserving. Since E^0A is a commutative primitive Hopf algebra, $A(PE^0A) = E^0A$ by Corollary 3.2, and similarly for $A(QA)$. Now $PE^0A \to QE^0A$ is just the composite

$$E^0_{-1,*}A(QA) = QA \xrightarrow{\sigma} IA \xrightarrow{\pi} QA = E^0_{-1,*}A$$

and is thus the identity. Therefore E^0f is an isomorphism of Hopf algebras and f is an isomorphism of algebras. □

The following immediate consequence of the previous theorem was the theorem of Hopf which initiated the study of Hopf algebras.

Corollary 4.2 (Hopf). *Let A be a connected, commutative, and associative quasi Hopf algebra such that $Q_nA = 0$ if n is even. Then $A \cong E(QA)$ as an algebra. In particular, the conclusion holds if $A_n = 0$ for all sufficiently large n.*

Proof. For the last statement, note that an even degree indecomposable would give rise to a polynomial subalgebra. □

If the coproduct is coassociative, we can strengthen the conclusion of the preceding corollary.

Corollary 4.3. *Let A be a connected commutative Hopf algebra such that $Q_nA = 0$ if n is even. Then $A \cong E(PA)$ as a Hopf algebra.*

Proof. By Corollary 3.2, it suffices to prove that $\nu : PA \to QA$ is an epimorphism. By Corollary 3.3, ν is a monomorphism and it suffices to prove that A is cocommutative. By Lemma 1.2, we may assume that A is of finite type. Then A^* is a primitive Hopf algebra and $P_nA^* = 0$ if n is even. Thus $[x, y] = 0$ if $x, y \in PA^*$ and A^* is commutative. Therefore A is cocommutative. □

We conclude with the following basic result. By Corollary 3.3, it is just a restatement of the connected case of Corollary 3.2.

Theorem 4.4. *Let A be a connected, commutative, and cocommutative Hopf algebra. Then $A \cong E((PA)^-) \otimes P((PA)^+)$ as a Hopf algebra.*

CHAPTER 4

Restricted Lie algebras and Hopf algebras in characteristic p

This chapter is precisely parallel to the previous one. We first introduce restricted Lie algebras and prove the PBW theorem for their universal enveloping algebras. We next show that primitive Hopf algebras in characteristic p are the universal enveloping algebras of their restricted Lie algebras of primitive elements. We then use this fact to study the algebra structure of commutative Hopf algebras in characteristic p.

Most of these results first appeared in Milnor and Moore [**?**], but with different proofs, and some go back to earlier work of Borel and Leray and Samelson; §4 is a corrected version of results in [**?**].

1. Restricted Lie algebras

In this section and the next, we work over a commutative ring R of prime characteristic p. Of course, either $2 = 0$ or 2 is invertible in R. As before, we let X^+ and X^- denote the R-submodules of even and odd degree elements of an R-module X, with the convention that $X^+ = X$ and $X^- = \{0\}$ if $\operatorname{char} R = 2$.

Definition 1.1. A restricted Lie algebra over R is a Lie algebra L together with a function $\xi : L^+ \to L^+$ with $\xi(L_n) \subset L_{pn}$, such that there exists an associative algebra A and a monomorphism of Lie algebras $j : L \to A$ such that $j\xi(x) = \xi j(x)$, where $\xi : A^+ \to A^+$ is the p^{th} power operation. A morphism of restricted Lie algebras is a morphism of Lie algebras which commutes with the "restrictions" ξ.

Lemma 1.2. *Let L be a restricted Lie algebra. Let $x \in L$, $y \in L_n^+$, $z \in L_n^+$ and $r \in R$. Define* $(\mathrm{ad} y)(x) = [x, y]$ *and, inductively,* $(\mathrm{ad} y)^i(x) = [(\mathrm{ad} y)^{i-1}(x), y]$. *Then the following identities hold.*

(i) $[x, \xi(y)] = (\mathrm{ad} y)^p(x)$

(ii) $\xi(ry) = r^p \xi(y)$

(iii) $\xi(y+z) = \xi(y) + \xi(z) + \sum_{i=1}^{p-1} s_i(y,z)$, *where $is_i(y,z)$ is the coefficient of a^{i-1} in the expression* $\mathrm{ad}(ay+z)^{p-1}(y)$*; here a is a degree zero indeterminant.*

Proof. Part (ii) is trivial. Consider the polynomial algebra $P[b,c]$ on two indeterminates b and c of the same degree n, where n is even if $\operatorname{char} R > 2$. We have the identities

(1) $(b-c)^p = b^p - c^p$ and
(2) $(b-c)^{p-1} = \sum_{i=0}^{p-1} b^i c^{p-1-i}$

Thus the same identities hold for two commuting elements in any R-algebra. Embed L in an associative algebra A, as in the definition. Left and right multiplication by

y are commuting elements in the algebra $Hom_R(A, A)$, hence (1) implies (i) and (2) implies

(3) $(\mathrm{ad}y)^{p-1}(x) = \sum_{i=0}^{p-1} y^i x y^{p-1-i}$

To prove (iii), consider the polynomial algebra $A[a]$. Write

(4) $(ay + z)^p = a^p y^p + z^p + \sum_{i=1}^{p-1} s_i(y, z)a^i$.

We must evaluate the coefficients $s_i(y, z)$, which a priori lie in A, as elements of L. Formal differentiation of (4) with respect to a, using $d(a^i) = ia^{i-1}$, gives

(5) $\sum_{i=0}^{p-1}(ay + z)^i y(ay + z)^{p-1-i} = \sum_{i=1}^{p-1} is_i(y, z)a^{i-1}$.

Replacing x and y by y and $ay + z$, respectively, in (3) and comparing the result to (5), we find that $is_i(y, z)$ admits the description given in (iii). Setting $a = 1$ in (5), we obtain (iii). □

Observe that (iii) shows that $\xi(y + z) - \xi(y) - \xi(z)$ is in the sub Lie algebra of L generated by y and z.

We shall see that, at least if R is a field, any Lie algebra L with a restriction ξ satisfying these identities can be embedded in a restriction-preserving way as a sub Lie algebra of an associative algebra and is therefore a restricted Lie algebra. Of course, any associative algebra is a restricted Lie algebra under the commutator and p^{th} power operations.

Definition 1.3. The universal enveloping algebra of a restricted Lie algebra L is an associative algebra $V(L)$ together with a morphism of restricted Lie algebras $i : L \to V(L)$ such that, for any morphism of restricted Lie algebras $f : L \to A$, where A is an associative algebra, there exists a unique morphism of algebras $\tilde{f} : V(L) \to A$ such that $\tilde{f} \circ i = f$.

Clearly $V(L)$ is unique up to canonical isomorphism, if it exists.

Proposition 1.4. *Any restricted Lie algebra L has a universal enveloping algebra $V(L)$, and $i : L \to V(L)$ is a monomorphism whose image generates $V(L)$ as an algebra. Moreover, $V(L)$ is a primitively generated Hopf algebra.*

Proof. Let $I \subset U(L)$ be the two-sided ideal generated by all elements of the form $x^p - \xi(x)$, $x \in L^+$. Define $V(L) = U(L)/I$ and let $i : L \to V(L)$ be the composite of $i : L \to U(L)$ and the quotient map $U(L) \to V(L)$. The universal property is easily checked, and it is then clear that i is a monomorphism whose image generates $V(L)$. The proof of the last statement is exactly the same as for $U(L)$, the essential point being that $V(L \times L')$ is isomorphic to $V(L) \otimes V(L')$ for restricted Lie algebras L and L'. □

2. The restricted Poincaré-Birkhoff-Witt theorem

We here obtain the Poincaré-Birkhoff-Witt theorem for restricted Lie algebras L. The Lie filtration of $V(L)$ is defined exactly as was the Lie filtration of $U(L)$; see Definition 2.1 and the discussion following it. We shall describe the associated graded algebra $E^{\oplus}V(L)$ when L is R-free. In $V(L)$, $x^p = \xi(x)$ for $x \in L^+$. Since $\xi(x)$ has filtration one, $x^p = 0$ in the commutative algebra $E^{\oplus}V(L)$.

Let $L^{\sharp}$ denote the underlying R-module of L regarded as an abelian restricted Lie algebra with restriction zero and write $B(L) = V(L^{\sharp})$. Then $B(L) = A(L)/J$, where J is the ideal generated by $\{x^p | x \in L^+\}$. Clearly the inclusion of L in $E^{\oplus}V(L)$ induces a natural map of algebras $f : B(L) \to E^{\oplus}V(L)$.

THEOREM 2.1 (Poincaré-Birkhoff-Witt). *Let L be an R-free restricted Lie algebra. Then $f : B(L) \to E^{\oplus}V(L)$ is an isomorphism of Hopf algebras.*

PROOF. Give $B(L)$ its Lie filtration and $E^{\oplus}V(L)$ its filtration by filtration degree. Then $E^0B(L)$ is obtained by application of B to L regarded as a bigraded R-module via $L_{1,q} = L_{q+1}$, and $E^0E^{\oplus}(L) = E^0V(L)$. Since f is evidently a filtration-preserving epimorphism, it suffices to prove that E^0f is a monomorphism. Observe that the quotient maps $\pi : A(L) \to B(L)$ and $\rho : U(L) \to V(L)$ are filtration-preserving. Let $I = \ker \rho$. Recall the map of R-modules $\bar{\sigma} \colon U(L) \longrightarrow A(L)$ from the proof of Theorem 2.3. We shall construct a filtration-preserving morphism of R-modules $\tau : A(L) \to B(L)$ such that $\tau\bar{\sigma}(I) = 0$ and $E^0\tau = E^0\pi$. It will follow that $\tau\bar{\sigma} = \bar{\tau}\rho$ for a filtration-preserving R-map $\bar{\tau} : V(L) \to B(L)$ and that $E^0\bar{\tau}$ is a morphism of algebras. The composite

$$E^0B(L) \xrightarrow{E^0f} E^0V(L) \xrightarrow{E^0\bar{\tau}} E^0B(L)$$

will be the identity morphism of algebras, hence E^0f will be a monomorphism and the proof will be complete.

To construct τ, let $\{y_j\}$ be an R-basis for L^+. Clearly L^- plays a negligible role here, and we let x denote an arbitrary basis element of $A(L^-) = B(L^-)$ and define $\tau(x) = x$. Let z_j denote y_j regarded as an element of $B(L)$. We define τ by induction on the filtration degree. We define τ by the formulas

$$\tau(xy_{j_1}^{r_1} \dots y_{j_n}^{r_n}) = xz_{j_1}^{r_1} \dots z_{j_n}^{r_n} \text{ for each } r_i < p. \tag{2.2}$$

and

$$\tau(xy_{j_1}^{r_1} \dots y_{j_n}^{r_n}) = \tau(xy_{j_1}^{r_1} \dots y_{j_{i-1}}^{r_{i-1}}\xi(y_{j_1})y_{j_i}^{r_i - p}y_{j_{i+1}}^{r_{i+1}} \dots y_{j_n}^{r_n}) \text{ if } r_i \geq p. \tag{2.3}$$

By induction on the filtration degree, these formulas uniquely determine a well-defined filtration-preserving morphism of R-modules $\tau \colon A(L) \longrightarrow B(L)$ such that $E^0\tau = E^0\pi$. It remains to check that $\tau\bar{\sigma}(I) = 0$. By definition, I is the two sided ideal in $U(L)$ generated by $\{y^p - \xi(y) | y \in L^+\}$. If y is a linear combination $\sum k_i y_{j_i}$, the identities (ii) and (iii) of Lemma 1.2 and the agreement of commutators and Lie brackets of elements of L in $U(L)$ imply that

$$y^p - \xi(y) = \sum_i k_i^p(y_{j_i}^p - \xi(y_{j_i})).$$

Thus I is the two-sided ideal in $U(L)$ generated by $\{y_j^p - \xi(y_j)\}$. Now a calculation from the identity (i) of Lemma 1.2 and the inductive definitions of $\bar{\sigma}$ and τ gives the conclusion. □

The following corollaries are deduced precisely as in the case of Lie algebras.

COROLLARY 2.4. *Let $\{x_i\}$ and $\{y_j\}$ be R-bases for L^- and L^+ indexed on totally ordered sets. Then $V(L)$ is the free R-module on the basis*

$$\{x_{i_1} \dots x_{i_m} y_{j_1}^{r_1} \dots y_{j_n}^{r_n} | i_1 < \dots < i_m,\ j_1 < \dots < j_n \text{ and } 1 \leq r_k < p\}.$$

COROLLARY 2.5. *Let L be an R-free Lie algebra together with a restriction operation satisfying the identities listed in Lemma 1.2. Then L is a restricted Lie algebra.*

3. Primitively generated Hopf algebras in characteristic p

In this section, R is assumed to be a field of characteristic p. Again, all of the results remain valid if R is any ring of characteristic p and all R-modules in sight are R-free.

The R-module PA of primitive elements of a Hopf algebra A is a sub restricted Lie algebra. The universal property of $V(PA)$ thus gives a natural map of Hopf algebras $g : V(PA) \to A$, and g is an epimorphism if A is primitive. Let $\mathscr{RL}$ and $\mathscr{PH}$ denote the categories of restricted Lie algebras and of primitive Hopf algebras over R. We have functors $V : \mathscr{RL} \to \mathscr{PH}$ and $P : \mathscr{PH} \to \mathscr{RL}$, a natural inclusion $L \subset PV(L)$, and a natural epimorphism $g : V(PA) \to A$, where $L \in \mathscr{RL}$ and $A \in \mathscr{PH}$.

Theorem 3.1. *The functors $V : \mathscr{RL} \to \mathscr{PH}$ and $P : \mathscr{PH} \to \mathscr{RL}$ are inverse equivalences of categories. More explicitly,*

(i) $PV(L) = L$ for any restricted Lie algebra L and
(ii) $g : V(PA) \to A$ is an isomorphism for any primitive Hopf algebra A.

Proof. To prove (i), we consider the Lie filtration of $V(L)$. By the PBW theorem, $E^{\oplus}V(L) \cong B(L)$ as a Hopf algebra. Arguing precisely as in the characteristic zero case, we find that $PE^0V(L) = E^0_{1,*}V(L)$ and conclude that $PV(L) \subset F_1V(L)$. This proves (i). To prove (ii), consider the primitive filtration of A, as specified in the proof of Theorem 3.1. The Lie and primitive filtrations on $V(L)$ coincide and g is filtration-preserving. It follows just as in the characteristic zero case that E^0g is a monomorphism and that g is therefore an isomorphism. □

Corollary 3.2. *If A is a commutative primitive Hopf algebra such that $x^p = 0$ if $x \in (IA)^+$, then A is isomorphic as a Hopf algebra to $B(PA)$.*

Proof. $A \cong V(PA) \cong B(PA)$ since PA is an abelian restricted Lie algebra with restriction zero. □

Unlike its characteristic zero analog, Corollary 3.2 fails to describe arbitrary commutative primitive Hopf algebras A over R. We have $A \cong V(PA)$, and we shall study $V(PA)$ in more detail in the next section. For similar reasons, the characteristic p analog of Corollary 3.3 takes the following weaker form. We again emphasize that A was not assumed to be connected in the results above.

Corollary 3.3. *Let A be a connected quasi Hopf algebra.*

(i) $\nu : PA \to QA$ is a monomorphism if and only if A is associative and commutative and satisfies $x^p = 0$ for $x \in (IA)^+$.

(ii) If A is commutative and associative and if $\xi(A)$ is the sub quasi Hopf algebra of A whose positive degree elements are spanned by $\{x^p | x \in (IA)^+\}$, then the following is an exact sequence of R-modules.

$$\begin{tikzcd} 0 \arrow[r] & P\xi(A) \arrow[r] & PA \arrow[r, "\nu"] & QA \end{tikzcd}$$

(iii) If A is a commutative and cocommutative Hopf algebra, then the following is an exact sequence of R-modules.

$$\begin{tikzcd} 0 \arrow[r] & P\xi(A) \arrow[r] & PA \arrow[r, "\nu"] & QA \arrow[r] & Q\lambda(A) \arrow[r] & 0 \end{tikzcd}$$

Here $\lambda(A)$ is the quotient Hopf algebra $\xi(A^*)^*$ of A if A is of finite type and, in general, $\lambda(A)$ is the colimit of the $\lambda(B)$, where B runs over the sub Hopf algebras of A that are of finite type.

Proof. If ν is a monomorphism, then A is associative and commutative and $x^p = 0$ for $x \in (IA)^+$ by Lemma 1.1. Conversely, give A its product filtration, which is complete since A is connected. The previous corollary applies to give $E^0A \cong B(PE^0A)$. It follows as in the proof of Corollary 3.3 that ν is a monomorphism. To prove (ii), let $B = A//\xi A$. Then B satisfies the hypotheses of (i). By Theorem 2.3, we have the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & P\xi(A) \arrow[r] \arrow[d, "\nu"] & PA \arrow[r] \arrow[d, "\nu"] & PB \arrow[d, "\nu"] & \\
& Q\xi(A) \arrow[r] & QA \arrow[r] & QB \arrow[r] & 0
\end{tikzcd}$$

Here $\nu : PB \to QB$ is a monomorphism and $Q\xi(A) \to QA$ is zero. Now (ii) follows by a simple diagram chase. When A is of finite type, (iii) follows from (ii) by dualization, and the general case then results by passage to colimits. □

Corollary 3.4. *A sub Hopf algebra of a primitive Hopf algebra is itself primitive.*

Proof. Let $A \subset B$, where B is primitive. By precisely the same argument as in the proof of Corollary 3.4, it suffices to prove the result when A and B are connected. By Lemma 1.2, we may assume that A is of finite type. The proof of Lemma 1.2 applies to show that B is the colimit of its primitive sub Hopf algebras of finite type, and A will necessarily be contained in one of them. Thus we may assume that B is also of finite type. Then A^* is a quotient hopf algebra of B^*. Since $\nu : PB* \to QB*$ is a monomorphism, part (i) of the previous corollary applies to show that B^* is associative and commutative with zero p^{th} powers. Therefore A^* also has these properties and $\nu : PA \to QA$ is a monomorphism. Dualizing back, we have that $\nu : PA \to QA$ is an epimorphism. □

Corollary 3.5. *A sub Hopf algebra A of a primitive Hopf algebra B is a normal subalgebra if and only if PA is a restricted Lie ideal of PB. When this holds, $B//A = V(PB/PA)$ and*

$$0 \to PA \to PB \to P(B//A) \to 0$$

is an exact sequence of restricted Lie algebras.

Proof. The argument is the same as for Lemma 4.7, but with the observation that, since A is a subalgebra of B, PA is automatically closed under the restriction in B and is thus a restricted Lie ideal if and only if it is a Lie ideal. □

4. Commutative Hopf algebras in characteristic p

In this section, R is assumed to be a perfect field of characteristic p. We need R to be perfect since relations of the form $x^{p^q} = ry^p$, where r has no p^{th} root, would lead to counterexamples to the main results.

THEOREM 4.1. *Let A be a connected, commutative, and associative quasi Hopf algebra. For a morphism of R-modules $\sigma : QA \to IA$ such that $\pi\sigma = \mathrm{id}$, where $\pi : IA \to QA$ is the quotient map, let $R(A;\sigma)$ be the sub abelian restricted Lie algebra of A generated by the image of σ. For a suitable choice of σ, the morphism of algebras $f : V(R(A;\sigma)) \to A$ induced by the inclusion of $R(A;\sigma)$ in A is an isomorphism.*

PROOF. Clearly f is an epimorphism for any choice of σ. Let $\mathscr{F}$ be the family of pairs (B, σ), where B is a sub quasi Hopf algebra of A and $\sigma : QB \to B$ is a R-splitting of $\pi : B \to QB$ such that the following properties hold.

(1) The map of algebras $f : V(R(B;\sigma)) \to B$ associated to σ is an isomorphism.
(2) The map $QB \to QA$ induced by the inclusion of B in A is a monomorphism, and $(QB)_q = 0$ for $q > n$ if $(QB)_n \to (QA)_n$ is not an isomorphism.

Partial order $\mathscr{F}$ by $(C, \tau) < (B, \sigma)$ if $C \subset B$ and σ extends τ. Note that $QC \to QB$ is then a monomorphism such that $(QC)_q = 0$ for $q > n$ if $(QC)_n \to (QB)_n$ is not an isomorphism. The family $\mathscr{F}$ is non-empty since it contains $(R, 0)$, and the union of a chain in $\mathscr{F}$ is an element of $\mathscr{F}$. Therefore $\mathscr{F}$ has a maximal element (C, τ). Assume for a contradiction that $C \neq A$. Let n be minimal such that $(QC)_n \neq (QA)_n$. Then $(QC)_q = 0$ for $q > n$. Choose $y \in A_n$ such that $\pi(y)$ is not in QC and let B be the sub algebra of A generated by C and y; B is necessarily a sub quasi Hopf algebra. The quotient $B//C$ is a monogenic Hopf algebra with primitive generator the image z of y.

A check of coproducts shows that the minimal m such that $y^m = 0$ must be a power of p. Define the height of y by $\mathrm{ht}(y) = t$ if $y^{p^t} = 0$ but $y^{p^t-1} \neq 0$, or $\mathrm{ht}(y) = \infty$ if there exists no such t. It is possible that $y \in B$ has greater height than $z \in B//C$, but we claim that there exists $x \in B$ such that x also has image z in $B//C$ and $\mathrm{ht}(x) = \mathrm{ht}(z)$. Granting the claim, we complete the proof as follows. By Theorem 2.3, the composite map of algebras

$$\begin{tikzcd} C \otimes B//C \arrow[r, "i\otimes\sigma"] & B \otimes B \arrow[r, "\phi"] & B \end{tikzcd}$$

is an isomorphism, where $i : C \to B$ is the inclusion and $\sigma(z) = x$. If we extend $\tau : QC \to C$ to $\sigma : QB \to B$ by setting $\sigma\pi(y) = x$, then the associated map of algebras $V(R(B;\sigma)) \to B$ is an isomorphism and $(C, \tau) < (B, \sigma)$.

Thus it remains to prove the claim. There is nothing to prove if $p > 2$ and n is odd or if z has infinite height. Thus let $\mathrm{ht}(z) = s$. Let $C' = \xi^s(C)$. Since R is perfect, C' is a sub quasi Hopf algebra of C. Consider the commutative diagram

$$\begin{tikzcd} C \arrow[r] \arrow[d, "\gamma"] & B \arrow[r] \arrow[d, "\beta"] & B//C \arrow[d, "\alpha"] \\ C//C' \arrow[r] & B//C' \arrow[r] & (B//C')//(C//C') \end{tikzcd}$$

where the vertical arrows are quotient maps. By Corollary 2.4, α is an isomorphism, and we regard it as an identification. Let $x' \in B//C'$ map to $z \in B//C$. Then x' has height p^s. Indeed, $\xi^s(x')$ is primitive since $\psi(x') = x' \otimes 1 + u + 1 \otimes x'$, where $u \in I(C//C') \otimes I(C//C')$ and thus $\xi^s(u) = 0$. However, $B//C'$ has no non-zero primitive elements of degree $p^s n$ in view of the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & P(C//C') \arrow[r] & P(B//C') \arrow[r] & P(B//C) \end{tikzcd}$$

and the fact that all indecomposable elements of $C//C'$ have degree $\leq n$ and all $(p^s)^{th}$ powers of elements of $C//C'$ are zero (and similarly for $B//C$). Now choose $w \in B$ such that $\beta(w) = x'$. Then $\psi(w) = w \otimes 1 + v + 1 \otimes w$, where $v \in IC \otimes IC$. Since $(\mathrm{id} \otimes \beta)(v) \in IC \otimes I(C//C')$, $\xi^s(\mathrm{id} \otimes \beta)(v) = 0$. It follows that $(\mathrm{id} \otimes \beta)\psi\xi^s(w) = \xi^s(w) \otimes 1$. By Theorem 2.3, this implies that $\xi^s(w)$ is in C'. Let $\xi^s(w) = \xi^s(w')$, where $w' \in C$. If $x = w - w'$, then $\xi^s(x) = 0$ and x projects to z in $B//C$. □

Example 4.2. The theorem fails if σ is not chosen properly. For a counterexample, let $p = 2$ and take $A = P\{x\} \otimes E\{y\}$, where x and y are primitive elements of degrees one and three. If one foolishly defines $\sigma : QA \to A$ by $\sigma\pi(x) = x$ and $\sigma\pi(y) = y + x^3$, then $V(R(A;\sigma))$ is a polynomial algebra on two generators.[1]

We have the following immediate corollary for quasi Hopf algebras having only odd degree generators. We say that a commutative algebra is strictly commutative if $x^2 = 0$ for all odd degree elements x; of course, this always holds if $\mathrm{char}\, R \neq 2$.

Corollary 4.3. *Let A be a connected, strictly commutative, and associative quasi Hopf algebra such that $Q_n A = 0$ if n is even. Then $A \cong E(QA)$ as an algebra.*

Again, we obtain a stronger conclusion when the coproduct is coassociative.

Corollary 4.4 (Leray–Samelson). *Let A be a connected strictly commutative Hopf algebra such that $Q_n A = 0$ if n is even. Then $A \cong E(PA)$ as a Hopf algebra.*

Proof. This follows from Corollaries 3.2 and 3.3 by the same arguments used to prove Corollary 4.3. □

Using Corollary 3.5, we can obtain an analog of Theorem 4.4, but this result gives considerably less complete information than was obtainable in the characteristic zero case.

Corollary 4.5. *Let A be a connected, commutative, and cocommutative Hopf algebra over R, where $\mathrm{char}\, R > 2$. Let $B = E(PA^-)$ and $C = A//B$. Then $A \cong B \otimes C$ as a Hopf algebra.*

Proof. By (iii) of Corollary 3.3, $\nu : PA \to QA$ is an isomorphism in odd degrees. We may assume that A is of finite type. Dualizing, we have that $\nu : PA^* \to QA^*$ is also an isomorphism in odd degrees, and there results a map of Hopf algebras $\pi^* : B^* \to A^*$ such that the evident composite $B \to A \to B$ is the identity. Let $\rho : A \to C$ be the natural epimorphism and define $\omega : A \to B \otimes C$ to be the composite

$$\begin{tikzcd} A \arrow[r, "\psi"] & A \otimes A \arrow[r, "\pi\otimes\rho"] & B \otimes C. \end{tikzcd}$$

Since A is cocommutative, ψ and therefore also ω is a morphism of Hopf algebras. Since $(\epsilon \otimes \mathrm{id})\omega = \rho$ and $(\mathrm{id} \otimes \epsilon)\omega = \pi$, ω is clearly an epimorphism. Using the exact sequence of primitives in Corollary 3.5 and the fact that $P(B \otimes C) = PB \oplus PC$, we see that ω is an isomorphism on primitives and therefore a monomorphism. □

[1] This example is due to Paul Goerss.

To complete our results, we must still determine the structure of $V(L)$, where L is an abelian restricted Lie algebra. Clearly, it suffices to study L itself.

THEOREM 4.6. *Let L be an abelian restricted Lie algebra such that L_0 is finitely generated as a restricted Lie algebra. Then L is isomorphic to a direct sum of monogenic abelian restricted Lie algebras.*

PROOF. Clearly $L = L^- \times L^+$ as an abelian restricted Lie algebra. Since L^- is just a vector space, with no additional structure, we may as well assume that $L = L^+$. Let $L(n)$ be the sub abelian restricted Lie algebra of L generated by the L_i for $i \leq n$. Since L is the union of the $L(n)$, it suffices to prove the result when $L = L(n)$. We proceed by induction on n.

We first consider the case $L = L(0) = L_0$, which is exceptional. Let $P[t]$ denote the non commutative polynomial algebra in one indeterminate t with $tr = r^p t$ for $r \in R$. If $R = \mathbb{F}_p$, $P[t]$ is the ordinary polynomial algebra. The relation $\xi(rx) = r^p \xi(x)$ shows that L is a $P[t]$-module via $tx = \xi(x)$. Since R is perfect, $r \to r^p$ is an automorphism of R, and $P[t]$ is a principal ideal domain by Jacobson [**?**, p. 30]. Therefore, by [**?**, p. 43-44], every finitely generated $P[t]$-module is a direct sum of cyclic modules. This says that L is a finite direct sum of monogenic abelian restricted Lie algebras.

In general, L is the direct sum of $L(0)$ and its sub restricted Lie algebra of positive degree elements, so we may now assume that $L_0 = 0$. Consider the case $L = L(n)$, where $n > 0$ and the conclusion holds for $L(n-1)$. Choose a splitting σ of the epimorphism $L(n)_n \longrightarrow L(n)_n/L(n-1)_n$ and choose a basis for $L(n)_n/L(n-1)_n$. The image under σ of the chosen basis gives a set of generators of degree n of $L(n)$. Since, in contrast with the case $L(0)$, there is no further structure in sight in degree n, we may apply a passage to colimits argument to see that the conclusion holds in general if it holds when there are only finitely many generators, q say, of degree n. We proceed by induction on q, there being nothing to prove if there are no such generators. Thus assume first that L has q generators of degree n and let L' be the sub abelian restricted Lie algebra of L generated by $L(n-1)$ together with $q-1$ of these generators. Let $L'' = L/L'$. By the induction hypothesis, L' is a sum of monogenic abelian restricted Lie algebras. By construction, L'' is an abelian restricted Lie algebra generated by a single element, x say, of degree n. It suffices to prove that L is isomorphic to $L' \oplus L''$. To show this, it suffices to construct a morphism $f\colon L'' \to L$ of abelian restricted Lie algebras such that $\pi f = \mathrm{id}$, where $\pi : L \to L''$ is the quotient map.

Define the height of an element $z \in L$ by $\mathrm{ht}(z) = s$ if $\xi^s(z) = 0$ but $\xi^{s-1}(z) \neq 0$ and $\mathrm{ht}(z) = \infty$ if $\xi^m(z) \neq 0$ for all m. Of course, if $\pi(y) = x$, then $\mathrm{ht}(y) \geq \mathrm{ht}(x)$. To construct f, it suffices to find $y \in L$ such that $\pi(y) = x$ and $\mathrm{ht}(y) = \mathrm{ht}(x)$ since $f(x) = y$ then determines f. If $\mathrm{ht}(x) = \infty$, any y such that $\pi(y) = x$ will do. Thus assume that x has finite height s. Since R is perfect, $\xi^s(L')$ is a sub abelian restricted Lie algebra of L'. Let $M' = L'/\xi^s(L')$ and $M = L/\xi^s(L')$. We may identify L'' with M/M'. Choose $z \in M$ which projects to $x \in L''$ and $w \in L$ which projects to z. We have $M_t = 0$ for $t \geq p^s n$ by construction and $L''_t = 0$ for $t \geq p^s n$ since $\mathrm{ht}(x) = s$. Thus $M_t = 0$ for $t \geq p^s n$ and $\xi^s(z) = 0$. Therefore $\xi^s(w) = \xi^s(w')$ for some $w' \in L'$. Let $y = w - w'$. Then $\pi(y) = x$ and $\mathrm{ht}(y) = s$. □

Observe that $V(\oplus_i L_i) \cong \otimes_i V(L_i)$. One way to see this formally is to ignore the coproduct and observe that, as a left adjoint, the functor V from abelian restricted

Lie algebras to commutative algebras commutes with categorical coproducts, which are direct sums on the Lie algebra level and tensor products on the algebra level. The following two theorems are therefore direct consequences of Theorems 3.1 and 4.1. Note that a connected monogenic Hopf algebra is of the form $E[x]$, where $x \in (IA)^-$, or $P[x]/(x^{p^q})$ or $P[x]$, where $x \in (IA)^+$.

THEOREM 4.7. *If A is a primitive commutative Hopf algebra and A_0 is finitely generated as an algebra, then A is isomorphic as a Hopf algebra to a tensor product of monogenic Hopf algebras.*

THEOREM 4.8 (Borel). *If A is a connected, commutative, and associative quasi Hopf algebra, then A is isomorphic as an algebra to a tensor product of monogenic Hopf algebras.*